2012 WL 2568973
Only the Westlaw citation is currently available.
United States District Court,
S.D. New York.

Debra SCHATZKI and BPP Wealth, Inc., Plaintiffs,
v.
WEISER CAPITAL MANAGEMENT, LLC, Weisermazars, LLP and Hoitsz (a/k/a "Carijn") Michel, Defendants.

No. 10 Civ. 4685. | July 3, 2012.

Attorneys and Law Firms

Lawler Mahon & Rooney LLP, by: James J. Mahon, Esq., New York, NY, for Plaintiffs.

Stark & Stark, by: Scott I. Unger, Esq., Lawrenceville, NJ, for Defendants.

OPINION

SWEET, District Judge.

***1** Plaintiffs Debra Schatzki ("Schatzki") and BPP Wealth, Inc. ("BPP") (collectively, the "Plaintiffs") have moved pursuant to Rule 15 of the Federal Rules of Civil Procedure for leave to file a third amended complaint ("TAC") to add a sixth cause of action for violations of §§ 1030(a)(2), 1030(a)(4), 1030(a)(5)(c) and 1030(6)(A) of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), and a seventh cause of action for unjust enrichment against the defendants Weiser Capital Management, LLC ("WCM"), Weisermazars, LLP ("Weisermazars") and Hoitz (a/k/a Carijn) Michel ("Michel") (collectively, the "Defendants"). Based on the conclusions set forth below, leave to file a cause of action for violation of the CFAA is denied and leave to file a TAC containing a cause of action for unjust enrichment is granted without opposition.

Prior Proceedings

Prior proceedings and the facts in this action are described in the opinion of this court, dated January 19, 2012. *See Schatzki v. Weiser Capital Mgmt., LLC,* No. 10–4685, 2012 WL 169779 (S.D.N.Y. January 19, 2012).

The instant motion was heard and marked fully submitted on April 4, 2012,

The Applicable Standard

Pursuant to Rule 15(a)(2) of the Federal Rules of Civil Procedure, leave to amend a complaint shall be give "freely" when "justice so requires." Fed.R.Civ.P. 15(a)(2). "If the underlying facts or circumstances relied upon by a plaintiff may be a proper subject of relief, he ought to be afforded an opportunity to test his claim on the merits," *Williams v. Citigroup Inc.,* 659 F.3d 208, 213 (2d Cir.2011) (quoting *Foman v. Davis,* 371 U.S. 178, 182, 83 S.Ct. 227, 9 L.Ed.2d 222 (1962)).

However, "[a] district court has discretion to deny leave for good reason, including futility, bad faith, undue delay, or undue prejudice to the opposing party." *McCarthy v. Dun & Bradstreet Corp.,* 482 F.3d 184, 200 (2d Cir.2007); *see also AEP Energy Servs. Gas Holding Co. v. Bank of Am., N.A.,* 626 F.3d 699, 726 (2d Cir.2010) ("Leave to amend may be denied on grounds of futility if the proposed amendment fails to state a legally cognizable claim or fails to raise triable issues of fact."). In addition, an amendment to a pleading will be futile if a proposed claim could not withstand a motion to dismiss pursuant to Rule 12(b)(6). *Ricciuti v. N.Y.C. Transit Auth.,* 941 F.2d 119, 123 (2d Cir.1991).

The Allegations Of Damage or Loss Under The CFAA Are Inadequate

In the TAG, the Plaintiffs allege that they incurred damages and losses, sufficient to state a claim under the CFAA, due to: (1) the Defendants' use of SmartOffice to obtain information without authorization and exceeding her authorized access and (2) the trafficking of computer passwords which were used to access the Plaintiffs' SmartOffice database. (TAG ¶ 102). The Plaintiffs contend that this access "enabled Defendants to obtain valuable private and confidential information about Plaintiffs' clients to further the intended conversion," and that securing "the return of the information" resulted in damages and losses in an amount in excess of $5000.00. (*Id.* ¶¶ 105, 106, 107).

***2** The CFAA provides that "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from

any protected computer ... shall be punished." 18 U.S.C. § 1030(a)(2)(C). The CFAA also subjects to criminal liability anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage." 18 U.S.C. § 1030(a)(5)(C).

While "the CFAA is primarily a criminal statute, § 1030(g) provides a civil cause of action in limited circumstances." *Garland–Sash v. Lewis,* No. 05–6827(WHP), 2012 WL 6188712, at *2 (S.D.N.Y. Dec. 6, 2011); *see* 18 U.S.C. § 1030(g). "The elements of a private cause of action under this statute are complex:

> a civil action under subsection 1030(g) of the CFAA requires; (1) establishing the elements of the particular substantive (criminal) offense under subsection 1030(a); (2) establishing that the plaintiff suffered "damage or loss" as a result of such a violation (although some, but not all, such offenses themselves already require "damage" and one now requires "damage and loss"); and (3) establishing one of the five types of conduct specified under subsection (c)(4)(A)(i), which are also required under subsection 1030(g) (some of which might also constitute "damage" or "loss")."

Nyack Hosp. v. Moran, No. 08–11112(SCR)(PED), 2010 WL 4118355, at *6 (S.D.N.Y. June 1, 2010) (internal citation omitted).

Thus, in order to bring a civil action, a plaintiff must show that she suffered "damage" or "loss" by a defendant's wrongful conduct. 18 U.S.C. § 1030(g) ("[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."). *Id.* In addition, any damage or loss must meet the $5,000.00 minimum statutory threshold. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

The CFAA narrowly defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Further, the statute defines "loss" as "a reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

While "physical damage to a computer is not necessary to allege damage or loss," *Bose v. Interclick, Inc.,* 10–9183(DAB), 2011 WL 4343517, at *3 (S.D.N.Y. Aug. 17, 2011), damages and losses are limited to "computer-related constructs." *Garland–Sash,* 2011 WL 6188712, at *3. Courts have recognized damages and losses to "computers, systems or data that could require economic remedy" as well as economic losses "bore in securing or remedying their systems" after an alleged CFAA. violation. *In re Doubleclick Inc. Privacy Litigation,* 154 F.Supp.2d 497, 524–25 (S.D.N.Y.2001). More specifically, a "loss" may include the costs of seeking to "identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to rescue the network." *Univ. Sports Pub. Co v. Playmakers Media Co .,* 725 F.Supp.2d 378, 383 (S.D.N.Y.2010).

***3** "Loss" is interpreted narrowly, however, and it "includes only costs actually related to computers." *Garland–Sash,* 2011 WL 6188712, at *4 (stating that "[n]othing in the CFAA suggests that the "loss" can be disassociated from the computer."). Courts in this district have rejected arguments that the statutory threshold for losses "includes the economic value of consumers' attention, that it includes the cost of business trips undertaken to respond to a computer hacking incident, or that it includes lost profits that are not attributable to an 'interruption of service.' " *B.U.S.A. Corp. v. Ecogloves, Inc.,* No. 05–9988(JSR), 2009 WL 3076042, at *6 (S.D.N.Y. Sept. 28, 2009) (internal citations omitted). In *In re Doubleclick Inc. Privacy Litigation,* for example, the Court stated that any allegations of injury involving "invasion of their privacy, [ ] trespass to their personal property, and [ ] misappropriation of confidential data, [are] not actionable because only economic losses are recoverable under 1030(g)." 154 F.Supp.2d at 525.

Here, the Plaintiffs failed to quantify any damages or loss that the Defendants' caused to their "computers, systems or data that could require economic remedy." *Id.* at 521. The TAG alleges that the Defendants obtained information without authorization and that they trafficked in computer passwords to the SmartOffice database. (TAC ¶ 102). The TAG also generally states that "[t]his access enabled Defendants to obtain valuable private and confidential information about Plaintiffs' clients to further the intended conversion" and that the "Plaintiffs were required to hire consultants and to incur legal fees, all in

an amount to be determined at trial" as a result of securing the return of the information. (*Id.* ¶¶ 105, 106).

The Plaintiff's CFAA claim might have been proper if, for example, it alleged that the Defendants' access to SmartOffice had damaged the data or the system itself, which caused the Plaintiffs to incur fees exceeding $5,000.00 to recover or restore it. The TAC does not allege, however, that the SmartOffice data at issue was destroyed or impaired, nor does it make any specific allegation as to the cost of identifying, securing or remedying the alleged damage caused by the access. *See Bose,* 2011 WL 4343517, at *4 (denying amendment to add a CFAA claim where plaintiff merely alleged that the defendant "impaired the functioning and diminished the value of [plaintiff's] computer in a general fashion" and "fail[ed] to make any specific allegation as to the cost of repairing or investigating the alleged damage to her computer."); *Fink v. Time Warner Cable,* No 08–9628(LTS)(KNF), 2009 WL 2207920, at *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because the plaintiff only alleged that the defendant caused damage by "impairing the integrity or availability of data and information," which was "insufficiently factual to frame plausibly the damages element of Plaintiff's CFAA claim.").

***4** Accordingly, the Plaintiffs' claim is inadequate to meet the definition of damages and losses under the CFAA. Because the amendment to the pleading will be futile as the CFAA claim could not withstand a motion to dismiss, leave to file the proposed TAC with the CFAA claim is denied.

The Unjust Enrichment Claim is Unopposed

Under New York law, a claim of unjust enrichment "requires simply an allegation that (1) the defendant was enriched, (2) the enrichment was at the plaintiff's expense, and (3) the defendant's retention of the benefit would be unjust." *M'Baye v. World Boxing Ass'n.,* No. 05–9581(DC), 2006 WL 2090081, at *5 (S.D.N.Y. July 28, 2006). "The notion of unjust enrichment applies where there is no contract between the parties." *Maryland Cas. Co. v. W.R. Grace & Co.,* 218 F.3d 204, 212 (2d Cir.2000). Thus, generally, quasi-contractual relief, such as unjust enrichment, is not permitted when an express agreement exists that governs the dispute between the parties. *See Clark–Fitzpatrick, Inc. v. Long Island R.R. Co.,* 70 N.Y.2d 382, 388, 521 N.Y.S.2d 653, 516 N.E.2d 190 (1987) (citations omitted).

Here, the proposed TAG adequately pleads a claim for unjust enrichment by identifying an underlying benefit that was conferred upon the Defendants at the Plaintiffs' detriment. (TAC ¶¶ 110, 111, 112). In addition, even though the Plaintiffs bring breach of contract claims against the Defendants, the Plaintiffs' unjust enrichment claim survives as an alternative to the alleged breach of contract claims. *See Singer v. Xipto Inc.,* ——F.Supp.2d ——, 2012 WL 1071274, at *8 (S.D.N.Y. Mar. 20, 2012) (stating that "[w]hile a party generally may not simultaneously recover upon a breach of contract and unjust enrichment claim arising from the same facts, it is still permissible to plead such claims as alternative theories."); *Wilk v. VIP Health Care Servs., Inc.,* No. 10–5530(ILG)(JMA), 2012 WL 560738, at *5 (E.D.N.Y. Feb. 21, 2012) (noting that "while it is true that a claim for quantum meruit or unjust enrichment is precluded when a valid contract governing the same subject matter exists between the parties, a quantum meruit claim may be alleged alongside a breach of contract claim.").

In addition, no opposition to the proposed additional cause of action for unjust enrichment having been filed by the Defendants. Accordingly, the motion for leave to amend as to the unjust enrichment claim is granted.

Conclusion

Based upon the conclusions set forth above, the Plaintiffs' motion for leave to amend is denied as to the CFAA claim as the allegations of the violation are inadequate, and leave is granted to serve and file a TAG containing a cause of action for unjust enrichment.

It is so ordered.

All Citations

Not Reported in F.Supp.2d, 2012 WL 2568973

End of Document

2012 WL 4933314
Only the Westlaw citation is currently available.
United States District Court,
D. Kansas.

SPRINT NEXTEL CORPORATION, Plaintiff,
v.
The MIDDLE MAN, INC. and Brian K. Vazquez, Defendant.

No. 12–2159–JTM. | Oct. 16, 2012.

Attorneys and Law Firms

Catherine C. Whittaker, Joseph M. Rebein, Shook, Hardy & Bacon LLP, Kansas City, MO, David B. Esau, James B. Baldinger, Stacey K. Sutton, Carlton Fields, PA, West Palm Beach, FL, for Plaintiff.

Ginnie C. Derusseau, James J. Kernell, Erickson Kernell Derusseau & Kleypas, LLC, Leawood, KS, for Defendant.

MEMORANDUM AND ORDER

J. THOMAS MARTEN, District Judge.

***1** The court has before it the defendants' Motion to Dismiss or Strike (Dkt. No. 16). The defendants contend that (1) this court lacks subject matter jurisdiction because the contracts at issue require arbitration; (2) the Complaint lacks sufficient factual assertions to put the defendants on notice of the claim or allow them to respond; and (3) the court should strike several paragraphs of the Complaint, characterized by the defendants as "prolix and prejudicial." The plaintiff, Sprint Nextel Corp., argues that (1) subject matter jurisdiction is proper, and if arbitration is required, then this court should stay the proceedings rather than dismiss them; (2) it has plead sufficient facts on all counts; and (3) the defendants have not made a proper showing to warrant granting the Motion to Strike. For the following reasons, the court denies the defendants' Motion.

I. Factual Background

Sprint Nextel Corp. claims that Brian K. Vazquez and his company The Middle Man, Inc. have been and are now engaged in an unlawful business practice that includes bulk purchase and resale of Sprint phones, theft of Sprint's subsidy investment in the phones, unlawful access of Sprint's protected computer systems and wireless network, trafficking of Sprint's protected and confidential computer passwords, and willful infringement of Sprint's trademarks.

Sprint alleges that the defendants acquire large quantities of Sprint phones (1) from Sprint and/or its authorized dealers, and (2) through soliciting other co-conspirators to purchase Sprint phones in large quantities for the defendants' benefit. Part of the defendants' scheme requires the original purchaser of each phone to break its service contract with Sprint by refusing to pay the bill or cancelling Sprint's services. According to Sprint, the defendants disable the manufacturer-installed software in the phones that would otherwise restrict the phones access exclusively to Sprint's wireless system. This "hacking" or "unlocking" allows the defendants to resell the phones at a premium without requiring its customers to sign up for a Sprint service contract.

Sprint buys its phones from the manufacturer and then sells the phones at a discounted price, subsidizing the discount. Sprint recoups this subsidy by restricting the phones through software so they may only be used on Sprint networks and requiring every phone purchaser to sign up for a contract. Sprint claims when defendants unlock the phones and resell them, the defendants are committing a theft by preventing Sprint from recouping its subsidy costs. Sprint alleges that the defendants sell the illegally unlocked phones as new and under the Sprint trademarks. Sprint also alleges that by reselling the phones in foreign countries where wireless providers do not subsidize mobile phones, the defendants are able to sell the phones at below-market prices that are substantially higher than those charged in the United States.

Sprint claims that the defendants make misrepresentations in order to induce Sprint to activate phones on its wireless telecommunications network, which gives defendants unauthorized access to Sprint's protected computer networks. Sprint claims that by purchasing and selling Sprint phones, the defendants are illegally trafficking in the confidential codes contained in the phones that allow access to Sprint's networks and facilitating the improper access of Sprint's telecommunications network.

*2 Sprint alleges that defendants' conduct causes Sprint to lose millions of dollars. Sprint asserts the following claims against defendants: Count I breach of contract; Count II common law unfair competition; Count III tortious interference with business relationships and prospective advantage; Count IV civil conspiracy; Count V unjust enrichment; Count VI conspiracy to induce breach of contract; Count VII common law fraud; Count VIII fraudulent misrepresentation; Count IX trafficking in computer passwords under 18 U.S.C. § 1030(a)(6); Count X unauthorized access under 18 U.S.C. § 1030(a)(5)(C); Count XI unauthorized access with intent to defraud under 18 U.S.C. § 1030(a)(4); Count XII federal common law trademark infringement and false advertising under 15 U.S.C. § 1125(a)(1)(A) and (B); and Count XIII contributory trademark infringement.

II. Motion to Dismiss for Lack of Subject Matter Jurisdiction

Federal courts have limited jurisdiction and may exercise their power only when specifically authorized to do so. *Castanedo v. Immigration Naturalization Serv.,* 23 F.3d 1576, 1580 (10th Cir.1994). Federal district courts have original jurisdiction of all civil actions arising under the constitution, laws, or treaties of the United States. 28 U.S.C. § 1331. Under Federal Rule of Civil Procedure 12(b)(1), a party may move for dismissal based upon a court's lack of subject matter jurisdiction. When analyzing a Rule 12(b)(1) motion to dismiss, the court presumes it lacks subject matter jurisdiction until the plaintiff can prove otherwise. *See Kokkonen v. Guardian Life Ins. Co. of Am.,* 511 U.S. 375, 377, 114 S.Ct. 1673, 128 L.Ed.2d 391 (1994) ("It is to be presumed that a cause lies outside [the court's] limited jurisdiction, [ ] and the burden of establishing the contrary rests upon the party asserting jurisdiction.").

Sprint alleges several violations of federal law, each of which gives this court jurisdiction under 28 U.S.C. § 1331. However, the defendants argue that the Terms & Conditions agreement at issue requires arbitration between the parties, destroying this court's jurisdiction. Sprint has filed a Notice of Filing Demand for Arbitration (Dkt.22), but defendants have refused to arbitrate (*See* Dkt. 26). As a result, defendants' argument that Sprint must attempt arbitration is moot. The Motion to Dismiss based on lack of subject matter jurisdiction is, therefore, denied.

III. Motion to Dismiss for Failure to State a Claim

Federal Rule of Civil Procedure 8(a)(2) provides that a complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." The complaint must give the defendant adequate notice of what the plaintiff's claim is and the grounds of that claim. *Swierkiewicz v. Sorema N.A.,* 534 U.S. 506, 512, 122 S.Ct. 992, 152 L.Ed.2d 1 (2002).

"In reviewing a motion to dismiss, this court must look for plausibility in the complaint.... Under this standard, a complaint must include enough facts to state a claim to relief that is plausible on its face.' " *Corder v. Lewis Palmer Sch. Dist. No. 38,* 566 F.3d 1219, 1223–24 (10th Cir.2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal,* 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (clarifying and affirming *Twombly's* probability standard). Allegations that raise the specter of mere speculation are not enough. *Corder,* 566 F.3d at 1223–24. The court must assume that all allegations in the complaint are true. *Twombly,* 550 U.S. at 589. "The issue in resolving a motion such as this is 'not whether [the] plaintiff will ultimately prevail, but whether the claimant is entitled to offer evidence to support the claims.' " *Bean v. Norman,* No. 008–2422, 2010 WL 420057, at *2, (D.Kan. Jan.29, 2010) (quoting *Swierkiewicz,* 534 U.S. at 511).

*3 In the case at hand, the court finds that the Complaint provides sufficient factual allegations to justify allowing the plaintiff to offer evidence in support of its claims. Each count asserted against defendant in the Complaint is sufficiently supported by the facts, as plead by Sprint. Furthermore, the Complaint gives the defendants adequate notice of Sprint's claims and the basis for them. *See Swierkiewicz,* 534 U.S. at 512. Sprint's Complaint did not simply list the elements of each claim and conclude they were met. *See Iqbal,* 556 U.S. at 678. The Complaint went well beyond an "unadorned, the-defendant-unlawfully-harmed-me accusation." *Id.* Rather, the Complaint first explained in detail the extent of the defendants' alleged misconduct and then established how that misconduct fits into the elements Sprint's claims.

Taking these alleged facts as true and viewing them in the light most favorable to the plaintiff, this court finds that each count listed in the Complaint is facially plausible. The defendants' Motion to Dismiss for failure to state a claim is, therefore, denied.

IV. Motion to Strike

Upon motion of a party or upon its own motion "the court may order stricken from any pleading any insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." FED. R. CIV. P. 12(f). Motions to strike, however, are disfavored. *Falley v. Friends University,* 787 F.Supp.2d 1255, 1257 (D.Kan. April 14, 2011). The court should decline to strike material from a pleading unless that material has no possible relation to the controversy and may prejudice the opposing party. *Id.*

Defendants argue that several paragraphs in the Complaint should be stricken because they are "prolix, [ ] conclusory, compound, irrelevant, and ambiguous allegations that are prejudicial to Defendants." (Dkt.16, pg.11–17). This court disagrees. The Complaint includes thirteen counts based on the same set of facts. Given the high pleading standards required by Rule 8 and the complexity of the claims, the Complaint is necessarily thorough rather than "prolix" and "compound." None of the paragraphs at issue were "completely unrelated to the controversy," and the defendants fail to show how they are prejudiced by the Complaint. *See Falley,* 787 F.Supp.2d at 1257. Therefore, the Motion to Strike is denied.

IT IS ACCORDINGLY ORDERED this 16th day of October 2012, that defendants' Motion to Dismiss or Strike (Dkt. No. 16) is denied for the reasons stated herein.

All Citations

Not Reported in F.Supp.2d, 2012 WL 4933314

End of Document

PL 98–473, October 12, 1984, 98 Stat 1837

UNITED STATES PUBLIC LAWS
98th Congress - Second Session
Convening January 23, 1984

DATA SUPPLIED BY THE U.S. DEPARTMENT OF JUSTICE. (SEE SCOPE)
Additions and Deletions are not identified in this document.

PL 98–473 (HJRes 648)
October 12, 1984

Joint Resolution making continuing appropriations for the fiscal year 1985, and for other purposes.

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I

That the following sums are hereby appropriated, out of any money in the Treasury not otherwise appropriated, and out of applicable corporate or other revenues, receipts, and funds, for the several departments, agencies, corporations, and other organizational units of the Government for the fiscal year 1985, and for other purposes, namely:

SEC. 101. (a) Such sums as may be necessary for programs, or activities provided for in the Agriculture, Rural Development and Related Agencies Appropriation Act, 1985 (H.R. 5743), to the extent and in the manner provided for in the conference report and joint explanatory statement of the Committee of Conference (House Report Numbered 98–1071), filed in the House of Representatives on September 25, 1984, as if such Act had been enacted into law.

(b) Such sums as may be necessary for programs, projects, or activities provided for in the District of Columbia Appropriation Act, 1985 (H.R. 5899), to the extent and in the manner provided for in the conference report and joint explanatory statement of the Committee of Conference (House Report Numbered 98–1088), filed in the House of Representatives on September 26, 1984, as if such Act had been enacted into law.

(c) Such amounts as may be necessary for programs, projects or activities provided for in the Department of the Interior and Agencies Appropriations Act, 1985, at a rate of operations and to the extent and in the manner provided as follow, to be effective as if it had been enacted into law as the regular appropriation Act:

An Act making appropriations for the Department of the Interior and related agencies for the fiscal year ending September 30, 1985, and for other purposes.

TITLE I — DEPARTMENT OF THE INTERIOR

BUREAU OF LAND MANAGEMENT

MANAGEMENT OF LANDS AND RESOURCES

For expenses necessary for protection, use, improvement, development, disposal, cadastral surveying, classification, and performance of other functions, including maintenance of facilities, as authorized by law, in the management of lands and their resources under the jurisdiction of the Bureau of Land Management, including the general administration of the Bureau of Land Management, $393,849,000.

CONSTRUCTION AND ACCESS

For acquisition of lands and interests herein, and construction of buildings, recreation facilities, roads, trails, and appurtenant facilities, $1,228,000, to remain available until expended.

PAYMENTS IN LIEU OF TAXES

For expenses necessary to implement the Act of October 20, 1976 (31 U.S.C. 6901–07), "97 Stat. 323, 324" $105,000,000, of which not to exceed $400,000 shall be available for administrative expenses.

"(m) False information and threats.".

SEC. 2015. "18 USC 31 note" This part shall become effective on the date of the enactment of this joint resolution.

CHAPTER XXI — ACCESS DEVICES AND COMPUTERS

SEC. 2101. This chapter may be cited as the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984". "18 USC 1001 note"

SEC. 2102. (a) Chapter 47 of title 18 of the United States Code as amended by chapter XVI of this joint resolution is further amended by adding at the end thereof the following:

"Section 1030. "18 USC 1030" Fraud and related activity in connection with computers

"(a) Whoever —
"(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, "42 USC 2014" with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;
"(2) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or
"(3) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;
shall be punished as provided in subsection (c) of this section. It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.
"(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
"(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.
"(c) The punishment for an offense under subsection (a) or (b)(1) of this section is —
"(1)(A) a fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and
"(B) a fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and
"(2)(A) a fine of not more than the greater of $5,000 or twice the value obtained or loss created by the offense or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and
"(B) a fine of not more than the greater of $10,000 or twice the value obtained or loss created by the offense or

imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

"(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

"(e) As used in this section, the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.".

(b) The table of sections at the beginning of chapter 47 of title 18 of the United States Code is amended by adding at the end the following new items:

"1030. Fraud and related activity in connection with computers.".

SEC. 2103. "18 USC 1030 note" The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution, concerning prosecutions under the sections of title 18 of the United States Code added by this chapter.

CHAPTER XXII

SEC. 2201. "29 USC 524a" Notwithstanding this or any other Act regulating labor-management relations, each State shall have the authority to enact and enforce, as part of a comprehensive statutory system to eliminate the threat of pervasive racketeering activity in an industry that is, or over time has been, affected by such activity, a provision of law that applies equally to employers, employees, and collective bargaining representatives, which provision of law governs service in any position in a local labor organization which acts or seeks to act in that State as a collective bargaining representative pursuant to the National Labor Relations Act "27 USC 167", in the industry that is subject to that program.

CHAPTER XXIII

SEC. 2301. (a) Subsection (a) of section 1963 of title 18 of the United States Code, as amended by chapter III of this title, is further amended by adding at the end the following: "In lieu of a fine otherwise authorized by this section, a defendant who derives profits or other proceeds from an offense may be fined not more than twice the gross profits or other proceeds."

(b) Section 1963 of title 18 of the United States Code, as amended by chapter III of this title, is further amended by striking out subsection (d).

(c) Section 1963 (m)(1) of title 18 of the United States Code, as amended by chapter III of this title, is further amended by striking out "for at least seven successive court days".

(d) Section 413(a) of title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, "21 USC 853" as amended by chapter III of this title, is further amended by adding at the end the following: "In lieu of a fine otherwise authorized by this part, a defendant who derives profits or other proceeds from an offense may be fined not more than twice the gross profits or other proceeds."

(e) Section 413 of title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, "21 USC 853" as amended by chapter III of this title, is further amended —

(1) by striking out subsection (d); and

(2) by redesignating subsections (e), (f), (g), (h), (i), (l), (m), (n), (o), and (p) as subsections (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), and (o) respectively.

(f) Section 413(n) of title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended by chapter III of this title, and as so redesignated by this chapter, is further amended by striking out "for at least seven successive court days".

SEC. 2302. Part D of title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended by chapter III of this title and this chapter, is further amended by adding at the end the following new section:

"ALTERNATIVE FINE

"SEC. 415. "21 USC 855" In lieu of a fine otherwise authorized by this part, a defendant who derives profits or other

proceeds from an offense may be fined not more than twice the gross profits or other proceeds.".

SEC. 2303. (a) Section 524 of title 28 of the United States Code, as amended by chapter III of this title, is further amended in subsection (c)(1) —

(1) by striking out "and" at the end of subparagraph (c);
(2) by striking out the period at the end of subparagraph (1) and inserting a semicolon in lieu thereof; and
(3) by inserting after subparagraph (D) the following:
"(E) for equipping for law enforcement functions of forfeited vessels, vehicles, and aircraft retained as provided by law for official use by the Drug Enforcement Administration or the Immigration and Naturalization Service; and
"(F) for purchase of evidence of any violation of the Controlled Substances Act or the Controlled Substances Import and Export Act.".

(b) Section 524 of title 28 of the United States Code, as amended by chapter III of this title, is further amended in subsection (c) —

(1) by inserting after paragraph (2) the following new paragraph:
"(3) Any amount under subparagraph (F) of subsection (c)(1) of this section shall be paid at the discretion of the Attorney General or his delegate, except that the authority to pay $100,000 or more may be delegated only to the respective head of the agency involved."; and
(2) by redesignating paragraphs (3) through (8) as (4) through (9) respectively.

SEC. 2304. Section 613(a) of the Tariff Act of 1930, as amended by chapter III of this title, is further amended —

(1) by striking out "and" at the end of subsection (a)(1);
(2) by striking out the period at the end of subsection (a)(2) and inserting a semicolon in lieu thereof;
(3) by inserting after paragraph (2) of subsection (a) the following:
"(3) for equipping for law enforcement functions of forfeited vessels, vehicles, and aircraft retained as provided by law for official use by the United States Customs Service; and
"(4) purchases by the United States Customs Service for evidence (A) of smuggling of controlled substances, and (B) of violations of the currency and foreign transaction reporting requirements of chapter 53 of title 31, United States Code, "31 USC 5301 et seq" if there is a substantial probability that the violation of these requirements are related to the smuggling of controlled substances";
(4) inserting after subsection (a) the following:
"(b) If the expense of keeping the vessel, vehicle, aircraft, merchandise, or baggage is disproportionate to the value thereof, and such value is less than $1,000, such officer may proceed forthwith to order destruction or other appropriate disposition of such property, under regulations prescribed by the Secretary of the Treasury.
"(c) Amounts under subsection (a) of this section shall be available, at the discretion of the Commissioner of Customs, to reimburse the applicable appropriation for expenses incurred by the Coast Guard for a purpose specified in such subsection."; and
(5) by redesignating subsections (b) through (f) as subsections (d) through (h) respectively.

TITLE III — PRESIDENT'S EMERGENCY FOOD ASSISTANCE ACT OF 1984

SHORT TITLE

SEC. 301. "7 USC 1728 note" This title may be cited as the "President's Emergency Food Assistance Act of 1984".

PART A — PRESIDENT'S EMERGENCY FUND

FINDINGS

SEC. 302. "7 USC 1728" The Congress finds that —

(1) acute food crises continue to cause loss of life, severe malnutrition, and general human suffering in many areas of the Third World, especially in sub-Saharan Africa;
(2) the United States continues to respond to these needs, as a reflection of its humanitarian concern for the people of the Third World, with emergency food and other necessary assistance to alleviate the suffering of those affected by severe food shortages;
(3) the timely provision of food and other necessary assistance to those in need is of paramount importance if the worst effects of such food crises are to be mitigated; and

PL 99–474, October 16, 1986, 100 Stat 1213

UNITED STATES PUBLIC LAWS
99th Congress - Second Session
Convening January 21, 1986

DATA SUPPLIED BY THE U.S. DEPARTMENT OF JUSTICE. (SEE SCOPE)
Additions and Deletions are not identified in this document.

PL 99–474 (HR 4718)
October 16, 1986

An Act to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act "18 USC 1001 note" of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION. — Section 1030(a)(2) of title 18, United States Code, is amended —
(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof;
(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),";
(3) by striking out the term "or" where it appears at the end of section 1030(a)(2) of title 18; and
(4) by adding after the term "financial institution" the following: "or of a card issuer as defined in section 1602(n) of title 15,".
(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE. — Section 1030(a)(3) of title 18, United States Code, is amended —
(1) to read as follows:
"(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;"; and
(2) by striking out the flush language after section 1030(a)(3) of title 18, United States Code, beginning with "It is not an offense" and all that follows through "use of the computer.".
(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES. — Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.
(d) NEW OFFENSES. — Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:
"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;
"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby —
"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) "18 USC 1029" in any password or similar information through which a computer may be accessed without authorization, if —

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE. — Section 1030(b) of title 18, United States Code, is amended —

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS. — Section 1030 of title 18, United States Code, is amended —

(1) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(2) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(3) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3) or (a)(6)" in lieu thereof;

(4) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(5) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(6) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(7) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(8) by adding at the end of subsection (c) the following:

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph."; and

(9) by deleting the term "(b)(1)" where it appears in the first line of section 1030(c) of title 18 and inserting in lieu thereof the term "(b)".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION. — Section 1030(e) of title 18, United States Code, is amended —

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

(4) by adding at the end thereof the following:

"(2) the term 'Federal interest computer' means a computer —

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means —

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971; "12 USC 2001 note"

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; "15 USC 78*o*" and

"(H) the Securities Investor Protection Corporation;
"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and
"(7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumberated in section 101 of title 5.".
(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION. — Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:
"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

Approved October 16, 1986.

LEGISLATIVE HISTORY — H.R. 4718 (S. 2281):
HOUSE REPORTS: No. 99–612 (Comm. on the Judiciary).
SENATE REPORTS: No. 99–432 accompanying S. 2281 (Comm. on the Judiciary).
CONGRESSIONAL RECORD, Vol. 132 (1986): June 3, considered and passed House. Oct. 1, S. 2281 considered and passed Senate. Oct. 3, H.R. 4718 considered and passed Senate, amended. Oct. 6, House concurred in Senate amendments.

PL 99–474, 1986 HR 4718

132 Cong. Rec. H3275-04, 1986 WL 779755
Congressional Record —- House of Representatives
Proceedings and Debates of the 99th Congress, Second Session
Tuesday, June 3, 1986

COMPUTER FRAUD AND ABUSE ACT OF 1986

Mr. HUGHES. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4718) to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes, as amended.

The Clerk read as follows:

H.R. 4718

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.-Section 1030(a)(2) of title 18, United States Code, is amended-

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof; and

(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE; USE OF COMPUTER EXCLUSION.-Section 1030(a) of title 18, United States Code, is amended-

(1) in paragraph (3), by striking out "knowingly" and inserting " intentionally" in lieu thereof;

(2) in paragraph (3), by striking out ", or having accessed" and all that follows through "prevents authorized use of, such computer";

(3) in paragraph (3), by striking out "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation" and inserting in lieu thereof "if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use"; and

(4) by striking out "It is not an offense" and all that follows through "use of the computer.".

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.-Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.-Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.-Section 1030(b) of title 18, United States Code, is amended-

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.-Section 1030 of title 18, United States Code, is amended-

(1) by striking out "(b)(1)" and inserting "(b)" in lieu thereof;

(2) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(3) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(4) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3), or (a)(6)" in lieu thereof;

(5) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(6) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(7) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(8) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(9) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection

(a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.-Section 1030(e) of title 18, United States Code, is amended-

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

(4) by adding at the end thereof the following:

"(2) the term 'Federal interest computer' means a computer-

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects such use; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means-

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934.

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; and

"(6) the term 'exceeds authorized access' means to access a compute with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.-Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the

United States.".

The SPEAKER pro tempore. Is a second demanded?

Mr. SHAW. Mr. Speaker, I demand a second.

The SPEAKER pro tempore. Without objection, a second will be considered as ordered.

There was no objection.

The SPEAKER pro tempore. The gentleman from New Jersey <Mr. HUGHES> will be recognized for 20 minutes and the gentleman from Florida <Mr. SHAW> will be recognized for 20 minutes.

The Chair recognizes the gentleman from New Jersey <Mr. HUGHES>.

Mr. HUGHES. Mr. Speaker, I yield myself such time as I may consume.

(Mr. HUGHES asked and was given permission to revise and extend his remarks.)

Mr. HUGHES. Mr. Speaker, I have moved to suspend the rules and pass the bill, H.R. 4718, the Computer Fraud and Abuse Act of 1986. It is with great pleasure and satisfaction that I rise in support of the bill before us. It was reported by voice vote by the Committee on the Judiciary on May 6, 1986. It is the culmination of 4 years of bipartisan work in the Congress.

During this thorough investigation it became clear that computer technology has brought us a long way in the past decade. However, computer technology-with all its gains-has left us with a new breed of criminal: The technologically sophisticated criminal who breaks into computerized data files. One element of this expanding group of electronic trespassers-the so-called hacker-is frequently glamorized by the media, perhaps because the image of the hacker is that of a bright, intellectually curious, and rebellious youth-a modern-day Huck Finn. The facts are these young thrill seekers are trespassers, just as much as if they broke a window and crawled into a home while the occupants were away. The hacker of today can become the white-collar crime superstar of tomorrow, and we must not glamorize our Huck Finns into John Dillingers.

While we need to be concerned about youthful hackers, they pale in significance in comparison to the computer sophisticated criminal who combines his technological skill with old-fashioned greed and criminal intent to rob banks or destroy business records or steal trade secrets. The tools of the trade are not Smith and Wesson, but IBM and Apple. However, in today's world of instant electronic transfer of funds, the result can be more far reaching-and harder for law enforcement to reach.

What can be done about these crimes? I believe government and industry have a dual responsibility: Industry must work to prevent such crimes, and government must be willing and able to prosecute when crimes occur. The legislation before us, I believe, will go a long way toward fulfilling the responsibility of Congress in this scenario.

At this juncture, I would like to bring special attention to my colleagues who have worked hard and effectively in this endeavor. The first is the gentleman from Florida, Mr. NELSON, who was the first to bring this subject to the attention of the House of Representatives and has been a constant champion and dedicated proponent of this important legislation. Also, the ranking Republican of the Subcommittee on Crime, Mr. MCCOLLUM, and Mr. SHAW, who have been invaluable in this bipartisan endeavor. I also would like to thank Senators TRIBLE and LAXALT for their assistance in developing this consensus bill. I appreciate their efforts in shepherding S. 2281, the companion bill to H.R. 4718, in the other body.

As many Members may recall, in the last Congress we enacted computer crime legislation as a part of the conference on the comprehensive crime bill. At the behest of our colleagues in the other body, we deleted from that legislation certain provisions of the House-passed credit card/computer crime bill dealing with felony theft and private-sector offenses involving misuse or damage involving computers. Since that time, both through the hearing process and informal negotiations with interested parties, we have attempted to develop a bill to perfect the existing law and fill the gaps we left as a result of that conference agreement.

The legislation before us today, I believe, will expand in an appropriate but limited manner the types of criminal misconduct involving computers that should be subject to Federal jurisdiction while at the same time leaving to State and local agencies their proper role in this national problem.

In doing so, this bill expands the existing protection of financial records in financial institutions to all customers rather than only to customers who are "individuals" or partnerships consisting of five or fewer partners. The bill would also delete coverage of authorized users of government computers from this portion of existing law and make subsection 1030(a)(3) a pure trespass provision. The improper modifications, destructions or disclosures by authorized users of Federal computers however, are presently violations of other laws such as the Privacy Act, trade secrets laws, 18 U.S.C. 1361, et cetera, and there are adequate administrative sanctions that can also be imposed on Federal employees. Government employees also will be subject to the new "intent to defraud" felony offense in 1030(a)(4). This solves a potential problem that the existing law might have a "chilling effect" on " whistleblowers."

The major impact of this bill is in its three new offenses. The first proposes a 5-year felony violation for unauthorized access to a "Federal interest computer" in furtherance of an intent to defraud. These computers are defined as computers used by the Federal Government or by financial institutions, or when the conduct involves computers in different States. The second new offense can be categorized as "a malicious damage" felony violation in regard to Federal interest computers if there is $1,000 or more in damages.

The last new offense is a misdemeanor provision designed to proscribe the conduct associated with "pirate bulletin boards" used by hackers to display passwords to other persons' computers.

Having worked with experts on computer crime over the past several years, I believe the legislation passed in the last Congress along with the bill now being considered combined-with active efforts of industry to safeguard their property-will address the emergence of the computer criminal in our society.

Protection-both through law and technology-can and must be developed for the intangible property-information-which is the lifeblood of computer systems. Unless we act now to secure the "locks" and provide the laws, computer crime will be the crime wave of the next decade.

12:35 p.m.

It is a good bill, and I would be remiss if I did not thank our staff, Ed O'Connell in particular of the majority staff, and Charlene Heydinger of the minority staff, for their work over the past 6 months in developing this consensus legislation.

It is a good bill. It is a bill that I think will be effective in dealing with the computer criminal.

Mr. Speaker, I reserve the balance of my time.

The SPEAKER pro tempore. The gentleman from New Jersey <Mr. HUGHES> has consumed 7 minutes.

Mr. SHAW. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I would like first of all to compliment the chairman of the subcommittee, the gentleman from New Jersey <Mr. HUGHES>, as well as the ranking member, the gentleman from Florida <Mr. MCCOLLUM> and my friend and colleague, the gentleman from Florida <Mr. NELSON>, for the wonderful job that has been done on this bill, and also to add my congratulations to the members of the staff, as the chairman just did.

Mr. Speaker, The bill before us today, H.R. 4718, will send a strong message to Americans that computer crime is unacceptable and will be strictly punished. The current law regarding persons who access computers without authorization is enhanced by the provisions of this new bill.

H.R. 4718 protects Federal computers, bank computers, and computers used in interstate commerce. The bill provides a model for States to be used in developing local computer crime laws that would cover all other computers.

H.R. 4718 compliments current law by making it a crime to access a computer of the Federal Government or a financial institution. Penalties are also established for accessing a computer with intent to defraud the Federal Government, a financial institution, or a computer accessed by a second computer from a different State. Destruction of these computers is also prohibited. Finally, persons who traffic in the passwords used to gain unauthorized access to Federal Government computers will also be committing a crime.

This bill improves existing law and expands its coverage to include other serious computer crime activities. I urge the adoption of H.R. 4718.

Mr. Speaker, I reserve the balance of my time.

Mr. HUGHES. Mr. Speaker, I yield such time as he may consume to the distinguished gentleman from Florida <Mr. NELSON>.

Mr. NELSON of Florida. I thank the gentleman for yielding time to me.

Mr. Speaker, what a privilege for me to come to this point after years of interest in this subject matter, so that I can take the well of this House to thank the chairman of this subcommittee for his vision in understanding the problem of computer crime and then being able legislatively to do something about it.

The gentleman from New Jersey, the chairman of the subcommittee, is a man of extraordinary talent in the way that he can work in a bipartisan fashion and the way in which he can work with our colleagues in the other body and with the administration, specifically the Department of Justice, in fashioning a piece of legislation that will now flesh out the skeletal structure that was passed in 1984 into a complete piece of legislation that will become Federal law to address this problem of computer crime.

The gentleman from New Jersey spoke about the fact that we are confronting a new type of criminal today. It is not the kind of criminal who uses the crowbar, but a criminal who uses the computer keyboard, just as much an effective criminal, just as much a person who, in the old Latin term, uses the "mens rea," the criminal intent, and one who can do a great deal more damage than just breaking into the old safes of yesterday, one who can break into national security information, one who can break into the transactions of interstate commerce, one who can break into, indeed, the transactions of international commerce.

So it is a day of joy and happiness for me, after becoming involved with this subject matter 9 years ago when, then a member of the Legislature of the State of Florida, we passed the first computer crime law in the Nation-which then became a model for the other States. Most of the 50 States now have such laws on their books and now, thanks to the gentleman from New Jersey <Mr. HUGHES>, the chairman of the subcommittee, and his counterpart in the other body, Senator LAXALT, we will have a law on the Federal books that will give our prosecutors the tools that they need to go after this new, highly sophisticated type of criminal.

I just want to make reference to one other individual, not an individual who is in this body, but to a fellow who was at the time the chairman of the Florida Legislature Criminal Justice Committee, of which I was one of his subcommittee chairmen, who had the vision back in 1977 and 1978 to realize what potential this had for the Nation, and assigned the State legislation to me. His name is Ralph Haben, from Palmetto, FL, who then went on to become the speaker of the Florida House of Representatives. He is the one who had vision and gave me that opportunity to lead that successful legislative effort.

It is a happy day, and I thank the gentleman from New Jersey for his extraordinary leadership.

Today we are concerned with the broad problem of assuring the security and accuracy of computer operations in the financial and business heart of the Nation.

Computer-assisted crime is the way we should refer to this particular type of wrong-doing. But I doubt that the simpler, less accurate term "computer-crime" will disappear from popular reports of the problem.

Nevertheless, what we are talking about is not crimes committed by computers, but crimes committed by people with the assistance of computers. This includes crimes committed by people at a computer keyboard and crimes that take advantage of the ability of computer systems to bypass the human controls that existed in traditional accounting and auditing procedures.

The computer-assisted crime problem poses major difficulties for the future because computers will be increasingly available in our society to assist in whatever work we have to perform, and that means this power tool will be increasingly available for those criminal persons we always seem to have among us.

Computers may not commit crimes-any more than guns commit crimes. But we have to be realistic-there are people who will commit crimes with guns if they are readily available, and there are people who will commit crimes with computers as they become ubiquitous in our society. I doubt, frankly, that we can address the problem of crime by banning either. Americans may not now be as attached to their computers as they are to their guns, but I suspect they will be inseparable before too long.

It has been estimated that there are some 56,000 large general purpose computers and 213,000 smaller business computers in use by American businesses, universities and research organizations. Another 570,000 minicomputers and 2.4 million desktop computers are in use in the private sector.

The Federal Government, particularly the Pentagon and the Bureau of the Census, has many computers-more than 15,000 computers in the entire Federal establishment, including more than 3,000 in the Department of Defense.

I am sure there will be many more computers in government and business, and in our homes and schools, in the years ahead. I have direct experience in my own congressional office where we have a powerful minicomputer-with 256 K of core memory and 60 megabytes of disk memory, a tape drive for backups, and its own emergency power supply.

We were the test site for an advanced computer system designed for congressional correspondence. And our system demonstrates what is happening and will be happening in offices and institutions across the country.

More and more people are learning to use computers as a routine part of their work. In my office, we do not have a single computer operator who would preside over this mysterious new technology like the priest of some powerful but unknowable force.

From the receptionist to the administrative assistant, the computer is a daily working tool in my Washington office. We have also connected our district offices with our in-house computer, so the Florida staff members are able to handle correspondence and casework through the computer. They direct the computer to produce letters, either from standard letters or directly from the keyboard, and these come out in Washington in the daily stream of the letters that makes up a substantial part of a congressional office's daily work. The computer system also handles messages and memoranda back and forth and allows us to create and modify documents in Washington or Florida.

My point is not to talk about computerized office procedures. Rather, I am trying to emphasize-perhaps a little like preaching to the convinced-to emphasize that familiarity with computers is becoming the common experience of tens of millions of working Americans. And where people work daily with a powerful tool such as a computer, there will be those who go far beyond normal day-to-day use to overstep the boundaries between legitimate and criminal uses of these powerful devices.

It is estimated that there are more than 2 million computer operators, programmers, and technicians in the country. And I think this figure is far too low. It calculates primarily those who have a good deal of training in computer programming and operation, rather than the general use that is now becoming the norm for business and government offices.

Certainly the number of people familiar with computers outside of business and government is growing rapidly. It has been estimated that more than 6 million home computers are in use. This figure will explode in the next few years.

Moreover, these computers will increasingly be interfacing with the data banks of major institutions-banks, to direct the transfer of funds among the customers accounts; department stores, to order merchandise; TV polling operations, to get instant public reaction to public events, and many, many more.

So, granted that computers are becoming widespread in our society: Why should the Federal Government be involved? Why should theft and fraud and property damage be made Federal crimes when they involve computers?

Well, the Federal Government obviously has a direct interest when Federal agency computers are involved. The first electronic computer was designed for the military to calculate artillery trajectories in World War II. The first nonmilitary application-Univac I-was designed on contract for the Bureau of the Census. It cut the time for tabulating the 1950 census from more than 3 years to months-a remarkable achievement for the time. But Univac I was turned over to the Smithsonian as a museum piece in 1962. We have made considerable progress from those first vacuum-tube computers. With microchips, their capacity can virtually be held in your hand today.

The Defense Department has accepted the fact that computers are vulnerable to unauthorized penetration. Pentagon computers are compartmentalized so that a breach of security in one part will not enable an unauthorized person to access more than a small part of the total information in the system. Commercial computer systems have been developing similiar defenses against unauthorized users-along with programs to audit use to detect unauthorized use after it occurs.

It is also important that Government make its policy clear-that its computers and the computers systems vital to our national economy are not to be tampered with. This is one of the objectives of the legislation I am cosponsoring.

Federal legislation to strengthen the powers of Federal prosecutors to bring to justice those who illegally penetrate either the military or the civilian computers of the Federal Government obviously is in order.

Therefore, I urge passage of this legislation sponsored by my friend from New Jersey the chairman of the subcommittee. Enactment of this legislation into law will happily complete an 8-year effort to give U.S. attorneys a new Federal tool to prosecute this new type of criminal.

Mr. HUGHES. Mr. Speaker, will the gentleman yield to me?

Mr. NELSON of Florida. Certainly. I yield to the gentleman from New Jersey.

Mr. HUGHES. I thank the gentleman for yielding.

Mr. Speaker, I just want to thank the gentleman. Even though the gentleman is not a member of our Subcommittee on Crime, it was the gentleman from Florida who brought to my attention initially his great concerns over this area of criminal endeavor. I had not been sensitized to the extent of computer crime in this country because corporate America was very hesitant to come forward and tell just exactly what problems they had. They were embarrassed. They did not want to invite additional trespass on their data base. The gentleman from Florida worked extremely hard in the Flordia Legislature in developing the model for many States around the country to follow in the area of computer crime.

12:45 p.m.

I want to thank the gentleman for helping us lay the groundwork in the 98th Congress and working with us in this Congress to flush out the additional amendments that were needed to create an extraordinarily effective statute in my judgment. I want to thank the gentleman for that.

Mr. NELSON of Florida. The gentleman is very kind and I thank the gentleman for his leadership.

Mr. RODINO. Mr. Speaker, I rise in support of H.R. 4718, the Computer Fraud and Abuse Act of 1986. H.R. 4718 in general deals with what can be characterized as white collar crimes, which often are neglected both at the Federal and State levels. The prosecution of white collar crime, which silently robs millions of dollars from all of us, must remain in high priority for Federal law enforcement. It is in this perspective we must deal with computer fraud as we attempt to deter the theft of one of our most prized intangible commodities, information.

The Computer Fraud and Abuse Act of 1986 would accomplish this by setting up two new felonies, one involving any

fradulent theft and the other malicious damage of $1,000 or more caused by unauthorized access to a Federal interest computer. The bill, therefore, covers computers used by the Federal Government or financial institutions, or conduct involving computers in different States. The bill also would proscribe trafficking in computer passwords as a misdemeanor offense. This latter conduct is associated with what is called pirate bulletin boards.

In passing this legislation, I believe the Congress will be providing needed and appropriate protection to our computer resources and, hopefully, decrease future attempts by high technology criminals in our society. A report by a task force on computer crime of the section of criminal justice of the American Bar Association stated:

The annual losses incurred as a result of computer crime appear, by any measure, to be enormous. Over 25% (72) of the survey respondents report "known and verifiable losses due to computer crime during the last twelve months." The total annual losses reported by these respondents fall somewhere between $145 million and $730 million. Thus, the annual losses per respondent reporting losses could be anywhere from $2 million to as high as $10 million. Approximately 28% of the survey respondents reported no available system to monitor or estimate the value of their computer crime losses.

Federal law must keep pace with technology. It is as important today to develop Federal protection for intangible property such as computerized information as it was to develop Federal law to protect tangible assets in interstate commerce in the past. I commend the chairman of the Subcommittee on Crime, Mr. HUGHES, and the ranking subcommittee member, Mr. MCCOLLUM, for their fine work on this legislation, and I urge my colleagues to support it.

Mr. SHAW. Mr. Speaker, I have no requests for time, and I yield back the balance of my time.

Mr. HUGHES. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey <Mr. HUGHES> that the House suspend the rules and pass the bill, H.R. 4718, as amended.

The question was taken; and (two-thirds having voted in favor thereof), the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

64 Hastings L.J. 1447

Hastings Law Journal
June, 2013

Article
Special Issue on Circuit Splits

THE COMPUTER FRAUD AND ABUSE ACT AND DISLOYAL EMPLOYEES: HOW FAR SHOULD THE STATUTE GO TO PROTECT EMPLOYERS FROM TRADE SECRET THEFT?

Audra A. Dial and John M. Moye, Kilpatrick Townsend & Stockton LLP[a1]

This Article discusses the current split between the federal circuits over the scope of the Computer Fraud and Abuse Act ("CFAA") and whether it extends to employees who steal an employer's electronic trade secrets to which they were lawfully given access as employees. After discussing the legislative history of the CFAA and various appellate decisions interpreting its scope, the Authors argue that recent court decisions interpreting the statute--exemplified by the Fourth Circuit in WEC Carolina Energy Solutions, LLC v. Miller and the Ninth Circuit in United States v. Nosal--are unduly narrow in their scope.

The Authors argue that the CFAA, by its language, is broad enough to provide for civil liability when a disloyal employee misappropriates electronic trade secrets in violation of an employer's computer use policies. A contrary approach is harmful to employers and inconsistent with the statute's intent. In light of these ambiguities, clarification of the CFAA's scope--either from the Supreme Court or via legislative action--is sorely needed.

*1448 Table of Contents

Introduction

One of the many changes wrought by the digital revolution is that employers-- be they large companies, hospitals, or

government agencies--are storing more and more of their proprietary, sensitive information on electronic servers. Visit any employer's office today--large or small, in any industry, in any part of the United States--and the chances are high that their business documents, including customer lists, formulas, pricing data, personnel records, and financial records are maintained on electronic servers rather than in physical file cabinets. The employees who work at these offices no longer simply use email to communicate with each other; they also regularly access their employer's databases to review electronic documents and data, and they use this information in their regular course of business.

Growing access to electronic information has raised a related question: How can employers protect their most sensitive, electronically stored trade secrets (such as formulas, software code, or financial data)? Many employers require their employees to follow "computer use" policies that provide, for example, that the employee will not use the electronic information to which she has access for any improper or unauthorized purpose. But what happens if the employee violates those computer use policies and, while still employed, steals the employer's most sensitive electronic records?

For example, imagine that--in the course of her work day--an employee logs onto a password-protected company server, visits an electronic directory to which she has proper access (because of her position in the company), and steals thousands of the company's most sensitive files by transferring them to an external hard drive. Days later, that employee terminates her employment, hands off the external hard ***1449** drive to a competitor, and joins the competitor's operations to compete directly against the former employer using information obtained during her employment there. What remedies, if any, does the former employer have?

In addition to an action for trade secret misappropriation (assuming the information stolen involved a trade secret), the Computer Fraud and Abuse Act ("CFAA") has represented an additional method of enforcement in recent years.[1] That statute, originally passed in 1984, imposes both criminal and civil liability on a person who "intentionally accesses a computer without authorization" or "exceeds authorized access," thereby obtaining "information" from a computer that is "used in or affecting interstate or foreign commerce."[2] Until recently, the CFAA served as a powerful weapon in an employer's arsenal when the employer was faced with a deceptive employee who misappropriated electronic information in violation of the employer's computer use policies. In the last decade, companies have increasingly raised CFAA claims alongside state law claims for trade secret misappropriation in order to obtain federal court jurisdiction.[3]

More recently, however, it has become unclear whether and to what extent the CFAA remains a viable method of enforcing the theft of electronic information by internal employees. In WEC Carolina Energy Solutions, LLC v. Miller,[4] the Fourth Circuit Court of Appeals broadened the existing split between the federal circuits over whether the CFAA extends to rogue employees who misuse electronic information when the information was gained from a company computer to which the employee had proper access.

In WEC, the Fourth Circuit joined the Ninth and Second Circuits to hold that the CFAA cannot impose liability on an employee who was given lawful access to company information but later misused that information in violation of the employer's computer use policies.[5] Furthermore, the Fourth Circuit held that the CFAA can only impose liability on employees who are either not permitted to access certain company information but do so anyway, or who otherwise exceed the boundaries of their authorized access--perhaps by altering information in a computer beyond their access level.[6] However, the court made clear that the CFAA does not extend to an employee who has permission to ***1450** access certain electronic information and later misuses that information in violation of a company use policy.[7] This narrow interpretation of the statute contrasts with the Seventh, Fifth, and Eleventh Circuits, which have construed the CFAA as imposing liability in such circumstances.[8]

This circuit split--and the confusion over the scope of the phrases "exceeds authorized access" and "without authorization" in the statute--carries significant implications for all employers. First, the ability to pursue remedies under the CFAA against a misappropriating employee now depends in part on the jurisdiction in which the action is being pursued. Additionally, employers in those circuits that have taken a narrow approach will also be limited in their ability to pursue disloyal employees and will be required to take alternate measures to prevent the theft of their sensitive electronic information. Employers in these jurisdictions may be unable to obtain federal jurisdiction over trade secret misappropriation claims (absent diversity) when an employee steals electronic information from a company computer to which the employee had access. Whereas previously companies victimized by disloyal employees would typically use a federal CFAA cause of action alongside state causes of action like trade secret theft in order to obtain federal court jurisdiction,[9] that strategy may no longer

be viable in certain circuits.

This Article argues that the approach to the CFAA--exemplified by the Fourth Circuit in WEC --is unduly narrow in its scope, and that the type of conduct involved in WEC--a thieving employee who violated his employer's computer use policies and stole information to which he initially had "access"--is precisely the type of conduct that the CFAA was intended to prevent. At the very minimum, courts should recognize that the CFAA is broad enough to provide for civil liability when a disloyal employee misappropriates electronic information in contravention of the employer's computer use policies. An alternate, narrow view can be damaging to employers, as it could foreclose opportunities to obtain a remedy for disloyal conduct involving electronic information, particularly if such information does not rise to the level of a trade secret.

Part I of this Article explains the history of the CFAA and its purpose. Part II provides an overview of the existing circuit split, including the recent WEC decision. Part III argues that the approach taken by the Fourth, Ninth, and Second Circuits is unduly narrow in scope, is contrary to the intent of the CFAA, and can be harmful to employers. Part IV argues that clarification from the Supreme Court on the scope of the CFAA is sorely needed in light of the existing circuit split; the Court should recognize that the statute provides a civil remedy ***1451** in the case of a disloyal employee who misappropriates electronic trade secret information in violation of an employer's computer use policies.

I. The Computer Fraud and Abuse Act

Congress passed the CFAA in 1984.[10] The statute was the first piece of federal legislation to address computer crime.[11] Originally, the CFAA was intended to be an anti-hacking statute; it narrowly imposed criminal liability on persons who accessed a computer "without authorization" or "for purposes to which [the] authorization does not extend" in order to commit three specific types of acts: (i) obtain national security secrets; (ii) obtain personal finance records; or (iii) hack into federal government computers.[12]

Subsequent amendments, however, changed and significantly expanded the reach of the CFAA.[13] In 1994, Congress amended the CFAA to permit civil actions by persons who suffered "damage or loss by reason of a violation" of the statute.[14] In 1996, Congress again amended the statute so that it was no longer limited solely to particular types of digital information.[15] Congress also expanded the definition of "protected computer," which had originally been limited solely to "Federal interest" computers.[16] Today, the CFAA definition of "protected computer" broadly encompasses any computer "which is used in or affecting interstate or foreign commerce or communication."[17]

Advocates of both the broad and the narrow view of the phrase "exceeds authorized access" in the CFAA have cited the legislative history to support their argument.[18] Those in favor of the narrow view point out that Congress originally focused the Act to prevent computer hacking.[19] In addition, courts adopting a narrow view of the statute have relied on the 1986 Amendment to the CFAA, which eliminated references to the hacker's "purposes" in obtaining the information and replaced them with ***1452** the phrase "exceeds authorized access," suggesting that Congress continued to focus on computer hackers.[20] A 1996 Senate Report has also been interpreted to suggest that the CFAA is meant to prevent outside access to, not the misuse of, information.[21] Thus, advocates of the narrow view argue that, despite the broad language of the CFAA, it was drafted to prevent computer hacking, and that the legislative history does not suggest that Congress intended for the Act to apply more broadly to misappropriation by "inside" employees.

In contrast, defenders of the broad view assert that the legislative history of the CFAA just as strongly supports their position: The statute extends to disloyal employees who steal their employers' electronic information. These advocates point out that that the CFAA, although initially targeted at hackers, has been amended repeatedly and that each subsequent amendment has expanded the scope of the CFAA.[22] Indeed, Congress has expanded the CFAA to include a private civil cause of action where one did not initially exist, to apply to conduct well beyond the original, enumerated factors, and to expand the types of computers entitled to protection.[23] Proponents of this broad view assert that Congress intended the statute to cover a broad array of computer crimes. Moreover, as the type and scope of computer crimes have changed over the years as technology evolved and become more integral to businesses, Congress has broadened the CFAA to cover far more than traditional computer hacking by an "outsider."[24]

Federal courts have attempted to construe the purpose of the CFAA and the meaning of key elements in the act, namely "exceeds authorized access" and "without authorization," against this complex legislative ***1453** history. In doing so,

however, the courts have been unable to reach a clear consensus. Although the circuit split has been unfolding for years, the recent WEC decision has only exacerbated the disagreement among the circuits as to whether the CFAA extends to a disloyal employee who misappropriates the electronic trade secrets of her employer.[25]

II. The Present Circuit Split

A. The Fourth Circuit's Decision in WEC

WEC involved a fact pattern that is all too familiar in trade secret misappropriation cases. WEC, a company providing welding services to the power industry, sued its ex-employee Willie Miller, his assistant Emily Kelley, and their new employer Arc Energy Services, after Miller downloaded a large number of electronic files, abruptly resigned from his employment, and, along with Kelley, joined a competitor.[26]

During Miller's employment, he was provided a company laptop and had been granted access to the company's servers and intranet, which contained "numerous confidential and trade secret documents," including pricing terms, information on pending projects, and other technical information.[27] WEC had written policies in place prohibiting employees from (i) using any company information without authorization or (ii) downloading it to a personal computer.[28] However, WEC's computer use policies "did not restrict Miller's authorization to access the information."[29]

Miller resigned from WEC and joined Arc, a direct competitor.[30] While still employed by WEC, Miller downloaded a number of confidential documents from the company's servers and emailed them to his personal email account.[31] He and his assistant also "downloaded confidential information to a personal computer."[32] Each of these actions was taken solely to benefit Arc, Miller's future employer, rather than WEC.[33] Twenty days after leaving WEC, Miller "used the downloaded information to make a presentation on behalf of Arc to a potential WEC ***1454** customer," who ultimately awarded projects to Arc based upon the presentation.[34]

WEC sued in the U.S. District Court for the District of South Carolina, asserting nine state causes of action--including misappropriation of trade secrets, tortious interference with contract, and conversion--and a federal cause of action under the CFAA.[35] The district court dismissed the CFAA claim under Federal Rule 12(b)(6), finding that WEC's computer policies only limited the "use of information not access to that information."[36] The district court held that even if Miller and Kelley had acted "contrary to [WEC] company policies regulating use, [such conduct] would not establish a violation of company policies relevant to access, and, consequently, would not support liability under the CFAA."[37] In other words, the district court concluded that no liability was warranted under the CFAA because Miller had been permitted to access the information at issue as an employee.[38] The remaining state law claims were then dismissed for lack of subject matter jurisdiction.[39]

On appeal, a unanimous three-judge panel of the Fourth Circuit affirmed the district court's interpretation of the CFAA.[40] In its opinion, the court examined the scope of the CFAA and whether its provisions "extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access."[41] The court ultimately concluded that the phrases "without authorization" and "exceeds authorized access" as used in the statute mean that an employee cannot either "gain admission to a computer without approval" or gain information that is located "outside the bounds of his approved access."[42] The court declined to extend the CFAA to impose liability on employees for "the improper use of information validly accessed."[43] Because WEC gave Miller access to the information that he allegedly misappropriated, the Fourth Circuit concluded there was no basis for a CFAA violation (regardless of the purpose behind his access of the information).[44]

***1455** The Fourth Circuit raised concerns about reading the CFAA too broadly in light of the "rule of lenity" applicable in criminal law.[45] The court suggested that reading the CFAA more expansively could result in potential liability for any employee who "checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy."[46] Construing the statute as one "meant to target hackers," the court held that a broader view could transform the CFAA "into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."[47]

B. Other Circuits Following WEC's Narrow Approach to CFAA Liability

The WEC panel's decision was similar to that reached by the Ninth Circuit in the criminal case of United States v. Nosal.[48] Nosal involved a former employee of an executive search firm, Korn/Ferry International, who persuaded current employees of the firm to download confidential information from Korn/Ferry's computers and transfer the information to Nosal in order to help him start a competing business.[49] Although the employees had legitimate "access" to the employer's database and the confidential information contained therein, the company's internal computer use policies prohibited the unauthorized disclosure of such information.[50] The federal government filed criminal charges against Nosal under the CFAA, accusing him of "aiding and abetting the Korn/Ferry employees in 'exceed[ing their] authorized access' with intent to defraud."[51]

As in WEC, the Ninth Circuit's en banc Nosal decision addressed whether the phrase "exceeds authorized access" refers only to an employee who accesses files that the employee does not have permission to access, or whether it also penalizes an employee who has access to a computer by virtue of her employment but uses such data for unauthorized purposes.[52] The government argued that the language of the CFAA was broad in its scope and that the statute encompassed the improper use of electronic information.[53]

***1456** Specifically, the government noted that the phrase "exceeds authorized access" was defined to include accessing "a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[54] The government argued that the word "so" was defined in the CFAA as "in that manner," and that it referred to the manner in which the person accessing the information uses the information she obtains or alters.[55] According to the government, the word "so" (as defined) specifically referred to use, and a narrow reading of the statute would render the word "so" superfluous.[56] In addition, the government argued that this narrow reading ignored that the CFAA distinguished between two phrases: "without authorization" and "exceed authorized access."[57]

On appeal, the court recognized that the CFAA was "susceptible to the Government's broad interpretation" but ultimately found that the text, the rule of lenity, and the purpose of the statute supported the more restrictive interpretation.[58] The court therefore held that "the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'"[59]

Specifically, the Ninth Circuit focused on the fact that the statute was drafted to target hackers, and it read the phrase "exceeds authorized access" as applying to inside hackers (that is, those who may have some access to a company computer, but who go further and access--or "hack into"--files to which they have no authorized access).[60] The court also recognized that the "rule of lenity" is applicable to criminal statutes, explaining that if Congress meant for the CFAA to apply more broadly to protect electronic trade secrets, it would have used clearer language to signal its intent.[61] The court expressed concern with expanding criminal liability to conduct that, unlike hacking into a computer, is not "inherently wrongful."[62] Like the Fourth Circuit, the Ninth Circuit reasoned that a broad interpretation of the CFAA would mean that routine violations of employer computer use policies, such as "g-chatting with friends, playing games, shopping or watching sports highlights," could be transformed into potential criminal violations.[63] The court therefore concluded that ***1457** "exceeds authorized access" in the CFAA was "limited to violations of restrictions on access to information, and not restrictions on its use."[64] Because Nosal's accomplices had been afforded access to the company's information, the court found that the government failed to satisfy the element of "without authorization, or exceeds unauthorized access."[65]

Since Nosal in April 2012, a number of district courts in the Ninth Circuit have followed this interpretation of the CFAA.[66] In addition, although no other circuit courts have expressly adopted the narrow approach to the CFAA taken by the Ninth Circuit in Nosal and the Fourth Circuit in WEC, a number of district courts in other circuits have adhered to the narrow view of the statute with the expectation that their respective circuits will follow. For example, district courts in the Second Circuit have construed the phrases "without authorization" or "exceeds authorized access" similarly to Nosal.[67] Courts in the Sixth Circuit similarly appear poised to follow the approach taken by the Fourth and the Ninth Circuits.[68] ***1458** District courts in the Eighth Circuit[69] and the Third Circuit[70] have likewise endorsed the Nosal interpretation of the CFAA and the narrow reading of the phrases "without authorization" and "exceeds authorized access."

Consequently, these circuits will only impose liability under the CFAA when a disloyal employee accesses files that she has never been authorized to access. The mere misuse of electronically stored information (by passing information to a competitor, for example) will not satisfy the statutory threshold for civil liability under the CFAA if the employer gave the employee access to such information as part of her employment.

C. The Contrary View: Citrin and Its Progeny

In contrast, courts in other circuits have taken a broader approach to liability under CFAA, holding that where an employee exceeds the scope of his or her "authorized access" and downloads and misuses sensitive company files in contravention of the employer's use policies, such conduct will constitute "unauthorized access" under the statute.

The Seventh Circuit first adopted this approach in International Airport Centers v. Citrin.[71] That case involved a defendant, Citrin, who quit his job at International Airport Centers and started a competing business in violation of his employment contract.[72] Prior to returning his company laptop, he deleted all of the electronic data on the laptop--including data that he collected and data that would show that he engaged in improper conduct before he quit his job.[73] Citrin's former employer brought a civil action against Citrin under the CFAA, accusing Citrin of accessing "a protected computer without authorization," thereby causing damage to the company.[74]

On appeal of the district court's dismissal of the CFAA claims under Federal Rule 12(b)(6), Judge Posner wrote for the court that although Citrin had initially been given access to company information, he had ***1459** breached his duty of loyalty when he quit and started a competing business.[75] The court then held that when Citrin terminated his agency relationship with International Airport Centers, his "authority" to access the company laptop was also terminated.[76] Consequently, at the time Citrin deleted the files on his laptop, he no longer had "authorization" to access the laptop. Thus, the court held that Citrin acted "without authorization" in violation of the CFAA.[77]

On different facts, the Eleventh Circuit adopted a similarly expansive interpretation of the phrase "exceeds authorized access." In United States v. Rodriguez, the Eleventh Circuit upheld the imposition of criminal liability on a defendant who "obtained personal information [during his employment] for a nonbusiness reason."[78] The defendant, Rodriguez, worked as a representative for the Social Security Administration and had been given access to databases containing sensitive, confidential personal information--including any person's social security number, date of birth, address, and annual income.[79] The Administration's computer use policies expressly prohibited employees from obtaining personal information from the database without a legitimate business reason.[80] In violation of this policy, Rodriguez used the agency's database to obtain the personal records of seventeen individuals for decidedly nonbusiness reasons--specifically, to obtain personal information about women for whom he had romantic interests.[81] A jury found Rodriguez guilty of seventeen violations of the CFAA.[82]

On appeal, Rodriguez argued that his actions did not violate the CFAA because he "accessed only databases that he was authorized to use as a TeleService representative."[83] The Eleventh Circuit rejected his argument, holding that because the Social Security Administration's computer use policy authorized Rodriguez to obtain personal information only for actual business reasons, Rodriguez had "exceed[ed] authorized access" when he obtained personal information for nonbusiness reasons, thereby converting his otherwise permissible access into "unauthorized access."[84]

***1460** To reach this conclusion, the Eleventh Circuit explicitly distinguished an earlier Ninth Circuit decision, LVRC Holdings LLC v. Brekka,[85] in which the Ninth Circuit held that a former employee did not violate the CFAA when he emailed documents that he was authorized to access to his personal email account.[86] The Rodriguez court explained that in Brekka, there was no company policy prohibiting employees from sending email to personal accounts, whereas the Social Security Administration's policy clearly prohibited Rodriguez from obtaining personal information for nonbusiness reasons.[87] Thus, the terms of the employer's use policy were pivotal to the Eleventh Circuit's finding of criminal liability.

The Fifth Circuit has likewise taken a broad approach to liability under CFAA, holding in United States v. John that even "authorized access" to information may not be unlimited, particularly when the defendant uses his authorized access "in furtherance of or to perpetrate a crime."[88] In John, the defendant was a Citigroup employee with access to Citigroup's computer system and customer account information.[89] The defendant provided confidential customer information to her half-brother, who then fraudulently charged four different Citigroup customers' accounts.[90] A jury found the defendant guilty of two counts of "exceeding authorized access" to a protected computer under §1030(a)(2)(A) and (C) of the CFAA.[91]

On appeal, the defendant argued that she had access to Citigroup's computers and account information and that the CFAA prohibited only unauthorized access to protected computers, not unauthorized use of information.[92] The Fifth Circuit disagreed, finding that, although the defendant technically had access to the confidential information, Citigroup's computer use policies expressly limited her access to certain uses.[93] Using confidential information to assist in perpetrating a fraud was not included among the permitted uses, and thus the defendant's participation in a fraudulent criminal scheme exceeded her

permissible "access" to Citigroup's electronically stored information.[94]

The John court observed that the existence of Citigroup employee policies-- and John's knowledge of such policies--established the ***1461** parameters of her "authorized access."[95] Although the court recognized that violation of a confidentiality agreement should not always raise criminal charges, the court found that an employee's "access may be exceeded if the purposes for which access has been given are exceeded."[96] Given that the company's use policies prohibited the misuse of confidential information and that the defendant was aware of those policies, the court held that the defendant's actions--which involved the misuse of confidential information--violated the CFAA and satisfied the "exceed authorized access" element of §1030(a)(2).[97]

District courts in the Fifth, Seventh, and Eleventh Circuits have followed this broader approach to CFAA liability, recognizing that when an employee violates the terms of a computer use policy and engages in an impermissible use of electronic information, that employee will be deemed to have engaged in an "unauthorized" access of company information in violation of the CFAA. In the Fifth Circuit, for example, district courts have broadly interpreted the CFAA in both civil and criminal contexts.[98] Similarly, numerous district courts in the Seventh Circuit have found that an employee's breach of the duty of loyalty severs her authority to access the employer's information and exposes the employee to liability under the CFAA.[99] However, district courts in the Eleventh Circuit have not followed Rodriguez as consistently. At least one district court in that ***1462** circuit has recognized that the CFAA applies to an employee's misuse of information in violation of an employer's computer use policies.[100]

In summary, the federal circuits are significantly divided as to the scope of the CFAA and the extent to which otherwise permissible access to information can be construed as "unauthorized" to warrant the imposition of CFAA liability. The Fourth Circuit exacerbated this circuit split in WEC. As it now stands, courts in the Second, Fourth, and Ninth Circuits--as well as, perhaps, the Third, Sixth, and Eighth Circuits--have adopted the view that the CFAA does not extend to employees who have access to electronically stored trade secrets and company information, and who misuse that information in contravention of an employer's computer use policies. In contrast, the Fifth, Seventh, and Eleventh Circuits have adhered to the view that an employee's otherwise legitimate access can be rendered "unauthorized" when she exceeds the scope of the access given or otherwise engages in improper use of such information in violation of the employer's policies. Until the Supreme Court resolves this matter, the scope of the CFAA will depend largely on the location of the dispute involving misuse of electronic information.

III. What the Circuit Split Means for Employers and Their Electronic Trade Secrets

The circuit split over the scope of the CFAA has significantly impacted employers and their ability to prevent their employees' misuse of electronic information and trade secrets. Until recently, employers typically included a CFAA claim as a supplemental remedy--in addition to a state law claim for trade secret misappropriation--when faced with theft of electronic information.[101] Prior to the recent decisions narrowing its scope, the CFAA had been a useful tool in the arsenal of a trade secret plaintiff-- particularly as it allowed a party to obtain federal court jurisdiction over trade secret claims involving the theft of electronic trade secrets. Recently, however, the narrowing of the statute has negatively impacted employers: Not only does it drastically limit the ability to obtain federal court jurisdiction over trade secret claims, but it also places the onus on employers to anticipate and prevent the electronic ***1463** theft of information by their employees by narrowly defining each employee's ability to use company electronic information.

First, the narrow reading of CFAA has had the indirect effect of making it much more difficult to obtain federal court jurisdiction in cases of electronic trade secret misappropriation. Indeed, in WEC, the plaintiff brought a civil suit in federal district court in South Carolina, invoking federal jurisdiction under the CFAA.[102] After dismissing the CFAA claim, the court in WEC dismissed the remaining state law claims for lack of subject matter jurisdiction.[103] In doing so, the WEC panel seemed to recognize that its decision would foreclose the ability of plaintiffs (absent diversity) to bring claims involving theft of electronic trade secrets in a federal forum.[104] Thus, one harmful impact of the circuit split (and the narrow construction afforded to the CFAA by those circuits following WEC and Nosal) is that, at least in certain jurisdictions, a trade secret plaintiff will have to establish diversity jurisdiction to pursue relief for electronic trade secret theft in a federal forum or be forced to litigate these complex claims in a state court. This has made it much more difficult to pursue trade secret violations because local procedural rules vary and state case law lacks uniformity.

Moreover, employers operating in jurisdictions that have adopted a narrow approach to the CFAA will now be unable to protect their electronic trade secrets merely by implementing written computer use restrictions. The Fourth Circuit's WEC ruling makes clear that computer use restrictions are necessary but not sufficient to protect confidential electronic information because an employee's mere violation of a use restriction (such as the theft of electronic data) will not support CFAA liability if the employee's "access" to the data was otherwise permitted. Consequently, employers in these circuits will be forced to revamp their practices and take additional steps to protect their most sensitive electronic files, most likely by carving out and identifying a discrete set of employees who should be given access to categories of information, manually barring such access for all other employees, and changing access levels for employees when their job functions change. The narrow approach is very restrictive and essentially affords employers the opportunity to obtain civil liability only against employee "hackers."

The narrow approach also seems woefully inconsistent with the fundamental purpose of the CFAA, which was drafted to prohibit a range of acts of computer misuse (without regard to the type of information ***1464** stolen) and which, if anything, has been substantially broadened since its initial passage in 1984.[105] In light of technological developments in the nearly thirty years since its enactment, it seems inconsistent to read the CFAA as a narrow statute--designed only to penalize hacking--when the amendments to the statute suggest that it is intended to have a much broader application, particularly in the civil context. Moreover, the plain language of the statute--with two separate prongs, "without authorization" and "exceeds authorized access"--can be read broadly enough to encompass both the acts of rogue employees who "hack" into areas of the company to which they have no access (the "without authorization" prong) and the conduct of thieving employees who willfully violate their employer's computer use restrictions and thereby steal electronic data and information for an improper purpose (the "exceeds authorized access" prong).[106]

In light of the statutory language and intent--not to mention the detrimental impact that the narrow Nosal/WEC approach has on an employer's ability to prohibit the theft of its electronic trade secrets in a federal forum--the reasonable interpretation of the CFAA is the one articulated by Judge Posner in Citrin, which has been followed by the Fifth and Eleventh Circuits.[107] Under this view, an employee with access to information should be construed as having exceeded the scope of the access she was originally given when she engages in improper, unauthorized, or otherwise disloyal "use" of such information in violation of the employer's computer policies. In such cases, the proper approach is to construe the employee's access as being "unauthorized," given that the employer did not "authorize" its employee to engage in an improper theft or misuse of that information.

The contrary view--as reflected in WEC--renders civil CFAA actions of dubious efficacy for use by employers because it prohibits them from using the CFAA to prevent the internal electronic theft of information unless the employer anticipated the theft in the first place (such as by limiting access at the outset of the employment relationship). This renders the CFAA limited in reach, remedying only cases of external hacking.

Most importantly, the reasoning behind the narrow view of the CFAA focuses on concerns about proper notice to a potential defendant ***1465** facing criminal liability.[108] In the civil context, where the remedies available do not include loss of civil liberties, there is no similar policy concern that requires such a narrow construction. One possible way to "bridge the split" between the two circuits--either by Supreme Court intervention or by legislative amendment--would be to adopt the broader view of CFAA liability in the context of civil claims, while limiting criminal liability solely to those cases in which an individual is plainly not permitted to access certain information and nevertheless steals it via an act of computer hacking (either internal or external).

IV. Healing the Split: Why the Supreme Court Should Clarify the Scope of the CFAA

As noted above, the circuit split has exacerbated confusion over the scope of the CFAA and its effectiveness as a tool in cases involving disloyal employees. This confusion is problematic for employers who have to take additional measures to enforce their internal computer policies and to create more individualized policies for each employee. It also creates a notable lack of uniformity among the circuits in an important (and growing) area of the law. Moreover, in those jurisdictions taking a narrow approach to the CFAA, employers are effectively barred from pursuing a trade secret misappropriation action involving the theft of electronic trade secrets in a federal forum unless diversity jurisdiction is present.

The confusion over the scope and breadth of the CFAA has had serious implications beyond the employment arena. In

January 2013, for example, Aaron Swartz, a twenty-six-year-old Internet activist who was being prosecuted under the CFAA for allegedly hacking into an online academic database and downloading journal articles (not for economic gain), committed suicide on the eve of his trial.[109] His death prompted criticism, not only of the prosecutor who zealously pursued the charges under the CFAA, but also of the CFAA itself and its broad "unauthorized access" language; some even blamed Swartz's prosecution in part on the "extremely problematic" language of the CFAA.[110] In response, the House Judiciary Committee announced on January 24, 2013, that it intended to review the breadth of the CFAA, and Representative Zoe Lofgren (D-Cal.) proposed an amendment that would drastically narrow the scope of the CFAA.[111] Such criticism, however, ignored the fact that facing civil liability for an act has drastically different ramifications than does facing criminal liability, and the fair notice required to alert individuals to ***1466** potential criminal liability is much higher than the notice required for potential civil liability.[112] Moreover, this recent criticism over the vague language of the statute arguably offered a perfect opportunity for the Supreme Court to clarify the scope of the phrase "unauthorized access" in both the civil and criminal contexts.

Any immediate hopes that the Supreme Court might resolve the circuit split were dashed on January 2, 2013, when the Court issued an order denying the petition for a writ of certiorari filed by WEC in the wake of the Fourth Circuit's ruling.[113] Thus, for the time being, the split will remain between those jurisdictions--like the Fourth and Ninth Circuits--that take a narrow approach to the meaning of "exceeds authorized access" and those jurisdictions--like the Fifth, Seventh, and Eleventh Circuits--that take a more expansive approach to the CFAA. As a result, it will be imperative for employers to create more individualized computer use restrictions in order to attempt to protect the viability of a CFAA claim in any jurisdiction.

Conclusion

Unfortunately, so long as the circuit split remains, employers, practitioners, and courts alike will continue to lack guidance as to the scope of liability under the CFAA, particularly in cases of disloyal employees who violate computer use restrictions. It seems inevitable that the Supreme Court will again be asked to weigh in on the scope of the CFAA, perhaps when a circuit that is currently silent on this matter issues a ruling that aligns with the broader view of the CFAA. When that occurs, one can only hope that the Supreme Court will exercise its discretion and agree to step into the fray and resolve the circuit split. Until that time--at least in certain jurisdictions-- an employer's computer use restrictions that merely prohibit disloyal use of electronic information will be insufficient to protect confidential electronic information from internal employee theft under the CFAA.

Footnotes

a1 Ms. Dial is a partner in Kilpatrick Townsend's Technology Litigation Team, where she focuses her practice on litigating trade secret disputes and patent infringement matters. Mr. Moye is an associate on the firm's Technology Litigation Team. He is also an adjunct professor at the University of North Carolina School of Law, where he teaches a course focused on trade secrets law. The Authors would like to thank Jeffrey H. Fisher of Kilpatrick Townsend for his invaluable assistance in preparing this Article.

1 18 U.S.C. §1030 (2012).

2 Id. §1030(a)(2)(C).

3 See, e.g., Mobile Mark, Inc. v. Pakosz, No. 11-C-2983, 2011 WL 3898032 (N.D. Ill. Sept. 6, 2011) (bringing a claim for trade secret theft alongside a CFAA claim); AssociationVoice, Inc. v. AtHome Net, Inc., No. 10-CV-00109, 2011 WL 63508 (D. Col. Jan. 6, 2011) (same); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003) (same).

4 687 F.3d 199 (4th Cir. 2012).

5 Id. at 207.

6 Id. at 206.

7 Id. at 207.

8 See United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

9 See, e.g., WEC, 687 F.3d 199.

10 See H.R. Rep. No. 98-894 (1984), reprinted in 1984 U.S.C.C.A.N. 3689. "There is [n]o specific federal legislation in the area of computer crime." Id. at 3691.

11 Id.

12 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, §2102(a), 98 Stat. 2190, 2190-92 (1984) (codified at 18 U.S.C. §1030).

13 For a thorough discussion of each amendment to the CFAA, see Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1563 (2010).

14 Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097, 2098 (1994) (codified at 18 U.S.C. §1030(g)).

15 Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

16 Id. at 3492.

17 18 U.S.C. §1030(e)(2) (2012).

18 Thomas E. Booms, Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act, 13 Vand. J. Ent. & Tech. L. 543, 560-61 (2011).

19 See Briggs v. State, 704 A.2d 904, 911 (Md. 1998); Booms, supra note 18, at 560-61 (citing H.R. Rep. No. 98-894 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3706 ("[The CFAA] deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer.")).

20 US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009); see Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008).

21 Gast, 535 F. Supp. 2d at 966 ("Senate report[s have] suggested a difference between access without authorization and exceeding authorized access based on the difference between 'insiders' and 'outsiders.' Insiders were those with rights to access computers in some circumstances (such as employees), whereas outsiders had no rights to access computers at all (such as hackers)." (citing S. Rep. No. 104-357, 1996 WL 492169, at *4 (1996) and Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and

"Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1630 (2003)).

22 See Booms, supra note 18, at 560 (citing Guest-Tek Interactive Entm't Inc. v. Pullen, 665F. Supp. 2d 42, 45 (D. Mass. 2009) ("Although the majority of CFAA cases still involve 'classic hacking activities,' the CFAA's reach has been expanded in the past two decades by the enactment of a private cause of action and a more liberal judicial interpretation of the statutory provisions.")).

23 Id.; see P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, L.L.C., 428F.3d 504, 510 (3d Cir. 2005) ("[T]he scope of [[the CFAA's] reach has been expanded over the last two decades."); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) (quoting S. Rep. No. 104-357, at *7-8) ("The proposed §1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer.... This [section] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected.... The crux of the offense under §1030(a)(2)(C), however, is the abuse of a computer to obtain the information.").

24 Booms, supra note 18, at 560-61.

25 Compare WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206-07 (4th Cir. 2012), and United States v. Nosal, 676 F.3d 854, 862-63 (9th Cir. 2012), with Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

26 WEC, 687 F.3d at 202.

27 Id.

28 Id.

29 Id.

30 Id.

31 Id.

32 Id.

33 Id.

34 Id.

35 See WEC Carolina Energy Solutions, L.L.C. v. Miller, No. 0:10-CV-2775-CMC, 2011 WL 379458, at *5 (D. S.C. Feb. 3, 2011).

36 Id.

37 Id. (emphasis added).

38 Id.

39 Id. at *6.

40 See WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206-07 (4th Cir. 2012).

41 Id. at 203.

42 Id. at 204.

43 Id.

44 Id. at 207.

45 Id. The Ninth Circuit raised similar concerns in United States v. Nosal, 676 F.3d 854, 862-63 (9th Cir. 2012). Under the rule of lenity, "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." See U.S. v. LeCoe, 936 F.2d 398, 402 (9th Cir. 1991).

46 WEC, 687 F.3d. at 206.

47 Id. at 207.

48 676 F.3d 854 (9th Cir. 2012).

49 Id. at 856.

50 Id.

51 Id. (quoting 18 U.S.C. §1030(a)(4)).

52 Id. at 857.

53 Id.

54 Id. (quoting 18 U.S.C. §1030(e)(6)).

55 Id.

56 Id.

57 Id. at 856.

58 Id.

59 Id. (quoting Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)). Accord Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

60 Nosal, 676 F.3d. at 857.

61 Id.

62 Id. at 860.

63 Id.

64 Id.

65 Id. at 864. The Nosal case was remanded to the Northern District of California following the Ninth Circuit's ruling. On remand, the government moved forward with certain criminal charges against Nosal based on separate acts of "outsider hacking" that Nosal had allegedly committed unrelated to the CFAA charges based on the information to which Nosal had lawfully had access as an employee. See United States v. Nosal, CR-08-0237 EMC, 2013 WL 978226 at *6 (N.D. Cal. 2013). The United States argued that Nosal could be prosecuted under the CFAA for the "outsider counts"--in which former Korn/Ferry employees had hacked a current employee's password to access Korn/Ferry's "Searcher" database and had provided Nosal with confidential information. Id. The trial court allowed those charges against Nosal to proceed. Id. at *9. On April 24, 2013--following two days of jury deliberations--Nosal was convicted of the "outsider counts" under the CFAA. See Karen Gullo, Ex-Korn/Ferry Executive Convicted of Trade-Secret Theft, BloombergBusinessweek (Apr. 24, 2013), http://www.businessweek.com/news/2013-04-24/ex-korn-ferry-executive-convicted-of-trade-secret-theft-1. Nosal's conviction shows that the CFAA remains a helpful tool for employers faced with unauthorized acts of employee hacking, even if it is no longer viable in certain circuits as a means of preventing "inside" theft by employees with lawful access to information.

66 See Incorp Servs. Inc. v. Incsmart.Biz Inc., 11-CV-4660-EJD-PSG, 2012 WL 3685994, at *3 (N.D. Cal. Aug. 24, 2012) (citing Nosal and stating that "the CFAA is an anti-hacking statute, and not a misappropriation statute"); Hat World, Inc. v. Kelly, CIV. S-12-01591 LKK, 2012 WL 3283486, at *5 (E.D. Cal. Aug. 10, 2012) (same); see also Oracle Am., Inc. v. Serv. Key, L.L.C., C 12-00790 SBA, 2012 WL 6019580, at *5 (N.D. Cal. Dec. 3, 2012) (finding that using legitimate employee access for improper purposes is "beyond the scope of the CFAA" under Nosal).

67 See Major, Lindsey & Africa, L.L.C. v. Mahn, 10 CIV 4329 CM, 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010) (finding that the Second Circuit is likely to adopt the narrow view); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Jet One Grp. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980, 2009 WL 2524864, at *5-7 (E.D.N.Y. Aug. 14, 2009) (adopting the narrow view and stating that the "Second Circuit has implicitly adopted the narrow view").

68 See Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (suggesting that Ninth Circuit interpretation of CFAA was proper); Ajuba Int'l L.L.C. v. Saharia, No. 11-12936, 2012 WL 1672713, at *11-12 (E.D. Mich. May 14, 2012); ReMedPar, Inc. v. AllParts Med., L.L.C., 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933-36 (W.D. Tenn. 2008); Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008).

69 See Walsh Bishop Assocs., Inc. v. O'Brien, Civil No. 11-2673 DSD/AJB, 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) ("[S]ection (a)(2) is not based on use of information; it concerns access."); Xcedex, Inc. v. VMware, Inc., No. 10-3589, 2011 WL 2600688, at *4 (D. Minn. June 8, 2011) (adopting a narrow interpretation); Condux Int'l, Inc. v. Haugum, Civil No. 08-4824 (ADM/JSM), 2008 WL 5244818 (D. Minn. Dec. 15, 2008). But see NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) ("The Court concludes that the broad view can best distinguish between the CFAA's statutory language 'exceeds authorized access' and 'unauthorized access' by looking solely at the text of the statute.").

70 See Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009) ("The Court is persuaded by the reasoning in the latter line of cases, and adopts the less capacious view of the legal meaning of 'without authorization' and 'exceeds authorized access' expressed therein."); Brett Senior & Assocs., P.C. v. Fitzgerald, CIV.A. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007) ("The conduct targeted by section (a)(4), however, is the unauthorized procurement or alteration of information, not its misuse or misappropriation.").

71 440 F.3d 418 (7th Cir. 2006).

72 Id. at 419.

73 Id.

74 Id. at 420 (emphasis omitted) (quoting 18 U.S.C. §1030(a)(5)(A)(ii)).

75 Id. at 420-21.

76 Id. at 421 (quoting State v. DiGiulio, 835 P.2d 488, 492 (Ariz. Ct. App. 1992)) ("Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship.... Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.").

77 Id. at 420 (citing 18 U.S.C. §1030(a)(5)(A)(ii)).

78 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

79 Id. at 1260.

80 Id.

81 Id. at 1260-62 .

82 Id. at 1262 (citing 18 U.S.C. §1030(a)(2)(B)).

83 Id. at 1263.

84 Id. (emphasis added).

85 581 F.3d 1127 (9th Cir. 2009).

86 Id.

87 Rodriguez, 628 F.3d at 1263.

88 597 F.3d 263, 271 (5th Cir. 2010).

89 Id.

90 Id.

91 Id. at 269-70.

92 Id. at 271.

93 Id. at 271-72 .

94 Id. at 271 (citing United States v. Phillips, 477 F.3d 215, 218 (5th Cir. 2007)) (holding that a student who accessed part of a system to which he had not been given a password exceeded authorized use).

95 Id. at 272.

96 Id. (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001)).

97 Id.

98 See Barnstormers, Inc. v. Wing Walkers, L.L.C., No. EP-10-CV-261-KC, 2011 WL 1671641 (W.D. Tex. May 3, 2011) (citing John, 597 F.3d at 269) (holding that a defendant who was authorized to access a website as a member of the public violated the CFAA by using that access for the purpose of obtaining others' advertisements and placing copies of its advertisements on the site); Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028 (N.D. Tex. Apr. 20, 2011) (citing John, 597F.3d at 269) (holding that the use of information in violation of a restrictive covenant states a claim under the CFAA).

99 See Deloitte & Touche L.L.P. v. Carlson, No. 11 C 327, 2011 WL 2923865, at *4 (N.D. Ill. July 18, 2011) (citing Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006)) ("Here, Carlson is claimed to have begun his solicitation of Deckter before departing Deloitte. The data destruction was done, in part, to cover his tracks in wrongfully soliciting Deckter. If, as claimed, Carlson was so nakedly violating his Director Agreement, he would have been acting contrary to his employer's interests, thereby ending his agency relationship with Deloitte and making his conduct 'without authorization.'"); Jarosch v. Am. Family Mut. Ins. Co., 837 F. Supp. 2d 980, 1021 (E.D. Wis. 2011) ("The plaintiffs undeniably had authority to access American Family's customer information while acting on behalf of American Family. However, as previously found, the plaintiffs breached their respective duties of loyalty to American Family. Thus, the plaintiffs' breach of their respective duties of loyalty, namely their having taken American Family policyholder information for the benefit of their new insurance agencies, appears to have terminated their authority to access American Family's customer information."); Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 768 (N.D. Ill. 2009) ("Taking these allegations as true, as the Court must do at this stage of the case, Wu was allegedly accessing confidential Motorola computers to send Motorola's confidential information to its competitor's chief information

officer. This is sufficient to describe the accessing of Motorola's computers without or in excess of Wu's authorization, satisfying the requirement that Motorola allege that Wu's unauthorized access resulted in her obtaining information from Motorola's protected computers.").

100 See Amedisys Holding v. Interim Healthcare of Atlanta, Inc., 793 F. Supp. 2d 1302, 1315 (N.D. Ga. 2011) ("While there is some question of whether Plaintiff generally permitted Mack to send the Referral Logs to her personal email account, there is no question that Mack exceeded any authority she had when she sent them to herself after accepting a position at Interim for use in competing with Amedisys."). But see Trademotion, L.L.C. v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1290-91 (M.D. Fla. 2012) ("[T]he CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.").

101 See, e.g., Mobile Mark, Inc. v. Pakosz, No. 11-C-2983, 2011 WL 3898032 (N.D. Ill. Sept. 6, 2011) (bringing a claim for trade secret theft alongside a CFAA claim); AssociationVoice, Inc. v. AtHome Net, Inc., No. 10-CV-00109, 2011 WL 63508 (D. Col. Jan. 6, 2011) (same); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003) (same).

102 See WEC Carolina Energy Solutions, L.L.C. v. Miller, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *5 (D. S.C. Feb. 3, 2011).

103 Id. at *6.

炒Id. at

104 See WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206 n.4 (4th Cir. 2012) (noting that, although recourse under the CFAA for the alleged conduct was no longer available, "nine other state law causes of action potentially provide relief").

105 See Booms, supra note 18, at 560.

106 See P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, L.L.C., 428 F.3d 504, 510 (3d Cir. 2005) ("[T]he scope of [the CFAA's] reach has been expanded over the last two decades."); S. Rep. No. 104-357, 1996 WL 492169, at *7-8 (1996) ("[T]he proposed §1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer.... This [section] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected.... The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.").

107 Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

108 United States v. Nosal, 676 F.3d 854, 860-61 (9th Cir. 2012); WEC, 687 F.3d at 206.

109 See, e.g., Mike Scarcella, Hacking Defendant's Suicide Spurs Debate over Prosecutors, Fulton Cnty. Daily Rep., Jan. 16, 2013, at 9-10.

110 Id.

111 Juan Carlos Rodriguez, House Will Review CFAA After Pioneer Swartz's Death, Law 360 (Jan. 23, 2013, 6:30 PM), http://www.law360.com/articles/409186.

112 See, e.g., Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498-99 (1982) ("The Court has... expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe."); Barenblatt v. United States, 360 U.S. 109, 137 (1959) (Black, J., dissenting) ("For obvious reasons, the standard of certainty required in criminal statutes is more exacting than in noncriminal statutes. This is simply because it would be unthinkable to convict a man for violating a law he could not understand." (footnote omitted)).

[113] See WEC Carolina Energy Solutions, L.L.C. v. Miller, 133 S. Ct. 831 (2013) (denying cert.).

End of Document

Title: To amend title 18, United States Code, to protect Americans from cybercrime.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "International Cybercrime Prevention Act of 2015".

SEC. 2. TRADE SECRET THEFT ENFORCEMENT.

(a) In General.—Chapter 90 of title 18, United States Code, is amended—

(1) in section 1831(a), in the matter preceding paragraph (1), by inserting after "agent," the following: "or intending or knowing that the offense is committed at the request, under the direction, or on behalf of any foreign government, foreign instrumentality, or foreign agent,";

(2) in section 1832(b), by striking "$5,000,000" and inserting "the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided";

(3) in section 1835—

(A) by striking "In any prosecution" and inserting the following:

"(a) In General.—In any prosecution"; and

(B) by adding at the end the following:

"(b) Rights of Trade Secret Owners.—The court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential. No submission under seal made pursuant to this subsection may be used in a prosecution under this chapter for any purpose other than those set forth in this section. The provision of information relating to a trade secret to the United States or the court in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection, and the disclosure of information relating to a trade secret in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection unless the trade secret owner expressly consents to such waiver."; and

(4) in section 1839—

(A) in paragraph (1), by inserting "or foreign agent" after "government"; and

(B) in paragraph (3), in the matter preceding subparagraph (A), by inserting "strategies, negotiating positions," after "plans,".

(b) RICO Predicate Offenses.—Section 1961(1) of title 18, United States Code, is amended by inserting "sections 1831 and 1832 (relating to economic espionage and theft of trade secrets)," before "section 1951".

SEC. 3. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking "if—" and all that follows through "therefrom." and inserting "if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.".

SEC. 4. SERVICE ON FOREIGN DEFENDANTS.

Rule 4(c) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2), by adding at the end the following: "A summons may also be served at a place not within a judicial district of the United States using the procedures set forth in Rule 4(c)(3)(D)."; and

(2) in paragraph (3)—

(A) in subparagraph (C)—

(i) by inserting "at a place within a judicial district of the United States" after "organization";

(ii) by striking "A copy" and inserting "If the agent is authorized by statute and the statute so requires, a copy"; and

(iii) by striking "elsewhere in the United States" and inserting "in the or outside of the United States"; and

(B) by adding at the end the following:

"(D) A summons may be served on an organization at a place not within a judicial district of the United States:

"(i) by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process, in a manner authorized under the laws of the foreign jurisdiction where the officer or agent to be served is located; or

"(ii) by other means reasonably calculated to give notice, including—

"(I) a stipulated means of service;

"(II) a means that a foreign authority undertakes in response to a letter rogatory or letter of request;

"(III) a means that a foreign authority undertakes in response to a request submitted under an applicable international agreement; or

"(IV) a means otherwise permitted under an applicable international agreement.".

SEC. 5. PREDICATE OFFENSES.

Part I of title 18, United States Code, is amended—

(1) in section 1956(c)(7)(D)—

(A) by striking "or section 2339D" and inserting "section 2339D"; and

(B) by striking "of this title, section 46502" and inserting ", or section 2512 (relating to the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices) of this title, section 46502"; and

[(2) in section 1961(1), by adding "section 1030 (relating to fraud and related activity in connection with computers) if the act indictable under section 1030 is felonious," before "section 1084".]

SEC. 6. FORFEITURE.

(a) In General.—Section 2513 of title 18, United States Code, is amended to read as follows:

"2513. Confiscation of wire, oral, or electronic communication intercepting devices and other property

"(a) Criminal Forfeiture.—

"(1) IN GENERAL.—The court, in imposing a sentence on any person convicted of a violation of section 2511 or 2512, or convicted of conspiracy to violate section 2511 or 2512, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) such person's interest in any property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained or retained directly or indirectly as a result of such violation.

"(2) FORFEITURE PROCEDURES.—Pursuant to section 2461(c) of title 28, the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) thereof, shall apply to criminal forfeitures under this subsection.

"(b) Civil Forfeiture.—

"(1) IN GENERAL.—The following shall be subject to forfeiture to the United States in accordance with provisions of chapter 46 and no property right shall exist in them:

"(A) Any property, real or personal, used or intended to be used, in any manner, to commit or facilitate the commission of a violation of section 2511 or 2512, or a conspiracy to violate section 2511 or 2512.

"(B) Any property, real or personal, constituting or traceable to the gross proceeds taken, obtained, or retained in connection with or as a result of a violation of section 2511 or 2512, or a conspiracy to violate section 2511 or 2512.

"(2) FORFEITURE PROCEDURES.—Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section

981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.".

(b) Technical and Conforming Amendment.—The table of sections for chapter 119 is amended by striking the item relating to section 2513 and inserting the following:

"2513. Confiscation of wire, oral, or electronic communication intercepting devices and other property.".

SEC. 7. GIVING COURTS THE AUTHORITY TO SHUT DOWN BOTNETS.

(a) Amendment.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting "and abuse" after "fraud";

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking "or" at the end;

(ii) in subparagraph (C), by inserting "or" after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

"(D) violating or about to violate section 1030 where such conduct would affect 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing unwanted software on the computers, using the computers without authorization, or obtaining information from the computers without authorization;"; and

(B) in paragraph (2), by inserting ", a violation described in subsection (a)(1)(D)," before "or a Federal"; and

(3) by adding at the end the following:

"(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

"(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

"(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.".

(b) Technical and Conforming Amendment.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

"1345. Injunctions against fraud and abuse.".

SEC. 8. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) In General.—Chapter 47 of title 18, United States Code, is amended to by inserting after section 1030 the following:

"1030A. Aggravated damage to a critical infrastructure computer

"(a) Offense.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

"(1) of the operation of the critical infrastructure computer; or

"(2) of the critical infrastructure associated with such computer.

"(b) Penalty.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

"(c) Consecutive Sentence.—Notwithstanding any other provision of law—

"(1) a court shall not place any person convicted of a violation of this section on probation;

"(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

"(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

"(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

"(d) Definitions.—In this section

"(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

"(2) the term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).".

(b) Table of Sections.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

"1030A. Aggravated damage to a critical infrastructure computer.".

SEC. 9. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

(a) In General.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) by striking paragraph (2) and inserting the following:

"(2)(A) intentionally accesses a protected computer without authorization and thereby obtains information from or causes damage to any such protected computer;

"(B) accesses a protected computer with authorization and thereby knowingly obtains information from such computer that the accessor is not entitled to obtain, or knowingly obtains any information from such computer for a purpose that the accessor knows is prohibited by the computer owner, if—

"(i) the value of the information obtained exceeds [$10,000];

"(ii) [the conduct was undertaken in furtherance of any felony violation of the laws of the United States or of any State, unless an element of such violation would require proof that the information was obtained without authorization or in excess of authorization;] or

"(iii) the protected computer is owned or operated by or on behalf of a State or local governmental entity responsible for the administration of justice, public health, or safety, or of the United States Government; and

"(C) the limitation on access to or use of the information is not based solely on the terms of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, between a provider of online service and a customer or subscriber thereof;";

(B) in paragraph (5)—

(i) by striking "(A)"; and

(ii) by striking subparagraphs (B) and (C); and

(C) by striking paragraph (6) and inserting the following:

["(6) knowingly and willfully traffics in any password or similar information, or any other means of access, knowing or having reason to know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;";]

(2) in subsection (b), by inserting "for the completed offense" after "provided";

(3) in subsection (c)—

(A) in paragraph (1)—

(i) by striking "(A) a fine" and all that follows through "(B)"; and

(ii) by striking "which occurs" and all that follows through "this subparagraph";

(B) in paragraph (2)—

(i) in subparagraph (A)—

(I) by striking ", (a)(3), or (a)(6)"; and

(II) by striking "which does not occur" and all that follows through "this subparagraph;" and inserting "; and";

(ii) in subparagraph (B)—

(I) in the matter preceding clause (i)—

(aa) by striking "5" and inserting "10"; and

(bb) by striking "or an attempt" and all that follows through "subparagraph"; and

(II) in clause (iii), by striking "and" at the end; and

(iii) by striking subparagraph (C); and

(C) by striking paragraphs (3) and (4) and inserting the following:

"(3) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(3) of this section;

"(4) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

"(5)(A) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5), a fine under this title, imprisonment for any term of years or for life, or both;

"(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5), if the offense caused—

"(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

"(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

"(iii) physical injury to any person;

"(iv) a threat to public health or safety;

"(v) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

"(vi) damage affecting 10 or more protected computers during any 1-year period; or

"(C) a fine under this title, imprisonment for not more than 1 year, or both, for any other offense under subsection (a)(5);

"(6) a fine under this title or imprisonment for not more than 10 years, or both, in the case

of an offense under subsection (a)(6) of this section; and

"(7) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.";

(4) in subsection (e)—

(A) by striking paragraph (6) and inserting the following:

"(6) the term 'exceeds authorized access'—

"(A) means to access a computer with authorization and to use such access for a purpose that the accesor knows is prohibited by the computer owner, to include obtaining information that the accessor is not entitled to obtain; and

"(B) does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, between a provider of online service and a customer or subscriber thereof, if such violation constitutes the sole basis for determining that access to a protected computer is in excess of authorization;";

(B) by striking paragraph (10);

(C) by redesignating paragraphs (11) and (12) as paragraphs (10) and (11), respectively;

(D) in paragraph (10), as resdesignated, by striking "and";

(E) in paragraph (11), as redesignated, by striking the period at the end and inserting a semicolon; and

(F) by adding at the end the following:

"(12) the term 'willfully' means intentionally to undertake an act that the person knows to be wrongful;

"(13) the term 'online service' means an electronic communication service to the public (as defined in section 2510 of this title), a remote computing service (as defined in section 2711 of this title), or the provision to the public over the Internet of content or computing services; and

"(14) the term 'traffic' means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.";

(5) in subsection (g)—

(A) by striking "subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)" and inserting "clause (i), (ii), (iii), (iv), or (v) of subsection (c)(5)(B)"; and

(B) by striking "subsection (c)(4)(A)(i)(I)" and inserting "subsection (c)(5)(B)(i)";

(6) by striking subsection (i) and inserting the following:

"(i) Criminal Forfeiture.—

"(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any

other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) such person's interest in any property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

"(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section."; and

(7) by striking subsection (j) and inserting the following:

"(j) Civil Forfeiture.—

"(1) The following shall be subject to forfeiture to the United States and no property right shall exist in them:

"(A) Any personal property, real or personal, that was used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

"(B) Any property, real or personal, constituting or is derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

"(2) Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.".

(b) Technical and Conforming Amendment.—Section 7431(e)(3) of the Internal Revenue Code of 1986 is amended by striking "subparagraph (B)" and inserting "subparagraph (B)(iii)".